

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-207483

(P2000-207483A)

(43)公開日 平成12年7月28日(2000.7.28)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード ¹⁰ (参考)
G 0 6 F 19/00		G 0 6 F 15/28	B
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 D

審査請求 有 請求項の数30 ○L (全14頁)

(21)出願番号 特願平11-310468	(71)出願人 000004226 日本電信電話株式会社 東京都千代田区大手町二丁目3番1号
(22)出願日 平成11年11月1日(1999.11.1)	(72)発明者 藤岡 淳 東京都千代田区大手町二丁目3番1号 日 本電信電話株式会社内
(31)優先権主張番号 特願平10-320173	(72)発明者 阿部 正幸 東京都千代田区大手町二丁目3番1号 日 本電信電話株式会社内
(32)優先日 平成10年11月11日(1998.11.11)	(72)発明者 三浦 史光 東京都千代田区大手町二丁目3番1号 日 本電信電話株式会社内
(33)優先権主張国 日本 (JP)	(74)代理人 100066153 弁理士 草野 卓 (外1名)

(54)【発明の名称】電子投票方法、投票システム及びプログラム記録媒体

(57)【要約】

【課題】投票者が投票内容の暗号化に使用した鍵を集計者に送る必要をなくす。

【解決手段】投票者 v_i は投票内容 v_i を集計者Cの公開鍵 $k_{p,c}$ で暗号化し、その暗号化投票内容 x_i にタグ t_i を連結して z_i とし、 z_i を乱数 r_i で搅乱して前処理文 e_i を作り、その前処理文に対する署名 s_i と前処理文 e_i を選挙管理者Aへ送る。選挙管理者Aは前処理文 e_i に対するブラインド署名 d_i を作成して投票者 v_i へ返す。投票者はブラインド署名 d_i から乱数 r_i の影響を除去した選挙管理者の署名情報 y_i を得、投票データ $\langle z_i, v_i \rangle$ を集計者Cへ送る。集計者Cは選挙管理者の署名 y_i を検証し、合格したらデータ $\langle z_i, v_i \rangle$ を含む投票リストを作り、投票者に公開する。投票者 v_i はその投票リストを検査し、 z_i 中のタグ t_i が自分のものと一致するデータ $\langle z_i, v_i \rangle$ がリストにあることを確認する。集計者Cは z_i 中の x_i を復号化して投票内容 v_i を得、候補に対する投票数を集計する。

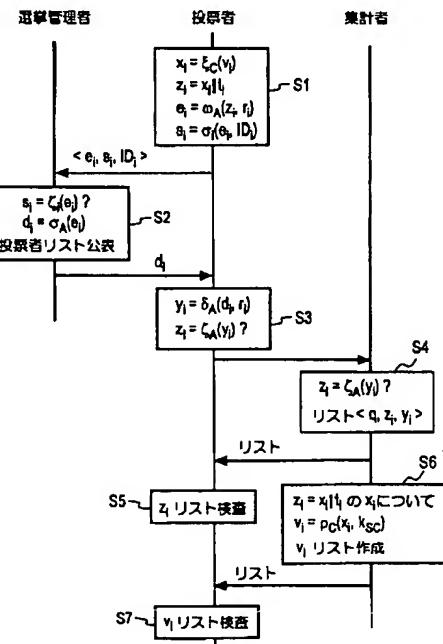


図6

【特許請求の範囲】

【請求項1】 管理者から投票の承認を得て投票者が集計者装置に投票データを送り、集計者装置が投票を集計する電子投票方法において、以下のステップを含む：

(a) 各投票者は、選択した候補に対応する投票内容を集計者装置の公開鍵を使って暗号化器により暗号化し、その暗号化投票内容を含む情報を乱数により攪乱して前処理文を作成し、管理者装置に送信し、

(b) 上記管理者装置は、各投票者装置の正当性を確認し、

受信した前処理文を署名作成器に入力して前処理文に対するブラインド署名を生成し、これを投票者装置に送り返し、

(c) 各投票者は、受信した前処理文に対するブラインド署名から上記乱数成分の影響を取り除き、

上記暗号化投票内容を含む情報に対する上記管理者の管理者署名を求め、その管理者署名と上記暗号化投票内容を含む情報を集計者装置へ投票データとして送信し、

(d) 上記集計者は、上記公開鍵に対応する秘密鍵を使って復号器により上記暗号化投票内容を含む情報を復号して投票内容を得て、上記投票内容に対応する候補の得票を集計する。

【請求項2】 請求項1の電子投票方法において、上記ステップ(d)に先立って、集計者が、受信した上記暗号化投票内容と上記署名情報を署名検査器に入力して前処理文が上記管理者によって署名されていることを確認し、暗号化投票内容を含む情報をリストを公表するステップ(d-0)と、上記投票者が、自分の暗号化投票内容が表に存在することを確認するステップ(d-1)とを更に含む。

【請求項3】 請求項1又は2の電子投票方法において、上記暗号化投票内容を含む情報を攪乱するステップ(a)は、上記投票者のみが知っているタグを生成するステップと、上記暗号化投票内容と上記タグを連結して上記乱数により攪乱するステップを含み、上記ステップ(d-1)は上記表中の投票データから上記タグを分離し、そのタグが自分のものであるかを検査するステップを含む。

【請求項4】 請求項1又は2の電子投票方法において、上記ステップ(b)は上記ブラインド署名を与えた投票者を表す情報のリストを投票者リストとして公表するステップを含み、上記ステップ(c)は上記投票者リストに自分を表す情報が含まれていることを確認するステップを含む。

【請求項5】 請求項1又は2の電子投票方法において、上記ステップ(d)は上記投票内容の集計結果を公表するステップを含む。

【請求項6】 請求項1又は2の電子投票方法において、上記ステップ(a)において上記投票者は上記前処理文に投票者識別情報を付けて上記管理者装置に送信し、

上記ステップ(b)において上記管理者は上記投票者識別情報を基づいて上記投票者を確認し、上記ステップ(c)において上記投票者は上記投票データを無記名で上記集計装置に送信する。

【請求項7】 請求項1又は2の電子投票方法において、上記ステップ(a)は上記投票分に対する投票者の署名を生成し、上記投票分と共に上記管理者装置に送信するステップを含み、上記ステップ(b)は上記投票分に対する上記投票者の署名の正当性を検査するステップを含む。

【請求項8】 請求項1の電子投票方法において、上記集計者装置は複数のシリーズ接続された分散集計者装置を有し、それぞれの分散集計者装置は異なる集計者により管理され、上記秘密鍵は上記複数の分散集計者装置に分割してそれぞれ分散秘密鍵として割り当てられており、上記ステップ(c)で各投票者は上記投票データを上記シリーズの一端の分散集計者装置に送信し、上記ステップ(d)は上記集計者装置がそれが備える復号処理部により上記分散秘密鍵を用いて上記暗号化投票内容を含む情報をシリーズに順次復号処理し、最終段の復号処理により上記投票内容を得るステップを含む。

【請求項9】 請求項1の電子投票方法において、上記集計者装置は複数の分散集計者装置を有し、それぞれの分散集計者装置は異なる集計者により管理され、上記秘密鍵は上記複数の分散集計者装置に分割してそれぞれ分散秘密鍵として割り当てられており、上記ステップ(c)で各投票者は上記投票データを全ての上記分散集計者装置に送信し、上記ステップ(d)は上記集計者装置がそれが備える復号処理部により上記分散秘密鍵を用いて上記暗号化投票内容を別々に復号処理して復号中間データを生成し、予め決めた1つの分散集計者装置に集め、復号処理をして上記投票内容を得るステップを含む。

【請求項10】 請求項8又は9の電子投票方法において、上記復号処理は、上記分散集計者装置の2以上の予め決めた数以上が動作をすれば復号可能な閾値付復号処理である。

【請求項11】 複数の投票者装置と、各上記投票者装置と記名通信路で接続された管理者装置と、各上記投票者装置と無記名通信路で接続された電子投票システムにおいて、

各上記投票者装置は、

投票内容を集計者装置の公開鍵で暗号化して暗号化投票内容を生成する暗号化器と、乱数を発生する乱数発生器と、

上記暗号化投票内容を上記乱数で攪乱して前処理文を作成する攪乱器と、

上記前処理文を上記管理者装置へ送信する手段と、

上記管理者装置から受信した上記管理者装置の上記前処理文に対するブラインド署名から上記乱数の影響を取り除いて上記暗号化投票内容を含む情報に対する上記管理

者装置の管理者署名を求める乱数成分除去器と、上記管理者署名と上記暗号化投票内容を含む情報を投票データとして集計者装置へ送信する手段とを含み、上記管理者装置は、受信した上記前処理文に対しブラインド署名を生成するブラインド署名作成器と、上記ブラインド署名を投票者装置へ送信する手段とを含み、

上記集計者装置は、

上記公開鍵に対応する秘密鍵により上記投票データ中の上記暗号化投票内容を含む情報を復号して上記投票内容を得る復号器と、上記復号された投票内容に基づいて候補に対する得票を集計する集計器とを含む。

【請求項12】 請求項11の電子投票システムにおいて、上記投票者装置は更に、上記暗号化投票内容を含む情報をに対する上記管理者署名を検証する管理者署名検査器を含み、その管理者署名検査器による検証に合格すると上記投票データを上記集計者装置へ送信し、上記集計者装置は各上記投票者装置から受信した上記投票データ中の上記暗号化投票内容を含む情報を上記管理者署名を入力して上記管理者署名を検証する管理者署名検査器を含む。

【請求項13】 請求項11の電子投票システムにおいて、上記投票者装置は更に上記前処理文に対する投票者署名を生成上記管理者装置へ送信する投票者署名作成器を含み、上記管理者装置は各投票者装置から受信した上記前処理文及びその投票者署名を検証する投票者署名検査器を含み、その検証に合格すると上記ブラインド署名作成器により上記ブラインド署名を作成する。

【請求項14】 請求項11の電子投票システムにおいて、上記集計者装置は上記管理者署名の検証に合格すると各上記投票者装置から受信した上記投票データのリストを投票リストとして作成し、上記投票者にアクセス可能に公表する投票リスト作成器を含み、上記投票者装置は上記集計者装置から受信した投票リストに自己の暗号化投票内容が存在するか否かを検査する投票リスト検査器とを含む。

【請求項15】 請求項14の電子投票システムにおいて、上記投票者装置は、上記投票者のみが知っているタグを生成するタグ発生器と、上記暗号化投票内容と上記タグを連結して上記暗号化投票内容を含む情報を生成する連結器と、上記投票リスト中の各投票データから上記タグを抽出し、そのタグが自分のものであるかを検査することにより自分の投票データが上記投票リストにあるかを検査するリスト検査部を含む。

【請求項16】 請求項11の電子投票システムにおいて、上記集計者装置はそれぞれ異なる集計者により管理される、複数のシリーズ接続された分散集計者装置を有し、上記秘密鍵は上記複数の分散集計者装置に分割して

10

20

30

40

50

それぞれ分散秘密鍵として割り当てられており、各上記投票者装置は上記投票データを上記シリーズの一端の分散集計者装置に送信し、上記分散集計者装置はそれぞれ割り当てられた上記分散秘密鍵を用いて上記暗号化投票内容を含む情報をシリーズに順次復号処理する復号処理部を有し、最終段の上記分散集計者装置における上記復号処理部の復号処理により上記投票内容を得る。

【請求項17】 請求項11の電子投票システムにおいて、上記集計者装置はそれぞれ異なる集計者により管理される複数の分散集計者装置を有し、上記秘密鍵は上記複数の分散集計者装置に分割してそれぞれ分散秘密鍵として割り当てられており、各上記投票者装置は上記投票データを全ての上記分散集計者装置に送信し、上記上記分散集計者装置はそれぞれ割り当てられた上記分散秘密鍵を用いて上記暗号化投票内容を別々に復号処理して復号中間データを生成し、予め決めた1つの上記分散集計者装置に送る復号処理部を有しており、上記予め決めた1つの上記分散集計者装置は集められた全ての上記復号中間データを復号処理して上記投票内容を得る統合復号部を有している。

【請求項18】 請求項16又は17の電子投票システムにおいて、上記復号処理部は、上記分散集計者装置の2以上の予め決めた数以上が動作をすれば復号可能な閾値付復号処理を行う。

【請求項19】 複数の投票者装置と、各上記投票者装置と記名通信路で接続された管理者装置と、各上記投票者装置と無記名通信路で接続された集計者装置を含む電子投票システムにおける、投票者装置であって、投票内容を集計者装置の公開鍵で暗号化し、暗号化投票内容を生成する暗号化器と、

乱数を発生する乱数発生器と、上記暗号化投票内容を含む情報を上記乱数により攪乱して前処理文を作成する攪乱器と、上記前処理文に対する投票者署名を生成する投票者署名作成器と、上記前処理文及びその投票者署名を管理者装置へ送信する手段と、

上記管理者装置から受信した、上記前処理文に対する管理者のブラインド署名と上記乱数を入力して上記ブラインド署名から上記乱数の影響を取り除いて上記暗号化投票内容を含む情報をに対する上記管理者の署名を求める乱数成分除去器と、

上記暗号化投票内容に対する上記管理者の署名と上記暗号化投票内容を含む情報を入力して、上記管理者の署名を検証する署名検査器と、

その署名検査器の検証に合格すると上記管理者の署名と上記暗号化投票内容を含む情報を投票データとして集計者装置へ送信する手段と、

上記集計者装置から受信した投票リストの中に自己の投票データが存在するか否かを検査するリスト検査部、と

を含む。

【請求項20】 請求項19の投票者装置において、更に上記投票者のみが知っているタグを生成するタグ発生器と、上記暗号化投票内容と上記タグを連結して上記暗号化投票内容を含む情報を生成する連結器とを含み、上記リスト検査部は上記集計者装置から受信した上記投票リスト中の各投票データから上記タグを抽出し、そのタグが自分のものであるかを検査することにより自分の投票データが上記投票リストの中にあるかを検査する。

【請求項21】 複数の投票者装置と、各上記投票者装置と記名通信路で接続された管理者装置と、各上記投票者装置と無記名通信路で接続された集計者装置を含む電子投票システムにおける、集計者装置であって、各上記投票者装置から投票データとして受信した、集計者の公開鍵で暗号化された暗号化投票内容を含む情報と上記暗号化投票内容を含む情報に対する管理者の署名とを入力して上記管理者の署名を検証する管理者署名検査器と、

上記管理者署名の検証に合格すると各上記投票者装置から受信した上記投票データのリストを作成し、上記投票者にアクセス可能に公表する投票リスト作成器と、上記公開鍵に対応する秘密鍵により上記暗号化内容を含む情報を復号して投票者の投票内容を得る復号器と、上記復号された投票内容に基づいて候補に対する得票を集計する集計器、とを含む。

【請求項22】 請求項21の集計者装置はそれぞれ異なる集計者により管理される、複数のシリーズ接続された分散集計者装置を有し、上記秘密鍵は上記複数の分散集計者装置に分割してそれぞれ分散秘密鍵として割り当てられており、各上記投票者装置から送られた上記投票データは上記シリーズの一端の分散集計者装置により受信され、上記分散集計者装置は、それぞれ割り当てられた上記分散秘密鍵を用いて上記暗号化投票内容を含む情報をシリーズに順次復号処理する分散復号処理部を有し、最終段の上記分散集計者装置における上記分散復号処理部の復号処理により上記投票内容を得る。

【請求項23】 請求項21の集計者装置はそれぞれ異なる集計者により管理される複数の分散集計者装置を有し、上記秘密鍵は上記複数の分散集計者装置に分割してそれぞれ分散秘密鍵として割り当てられており、各分散集計者装置は全ての上記投票者装置から上記投票データを受信し、割り当てられた上記分散秘密鍵を用いて上記暗号化投票内容を復号処理して復号中間データを生成し、予め決めた1つの上記分散集計者装置に送る分散復号処理部を有しており、上記予め決めた1つの上記分散集計者装置は集められた全ての上記復号中間データを復号処理して上記投票内容を得る統合復号部を有している。

【請求項24】 請求項22又は23の集計者装置において、上記分散復号処理部は、上記分散集計者装置の2

10

20

30

40

50

以上の予め決めた数以上が動作をすれば復号可能な閾値付復号処理を行う。

【請求項25】 複数の投票者装置と、各上記投票者装置と記名通信路で接続された管理者装置と、各上記投票者装置と無記名通信路で接続された集計者装置を含む電子投票システムにおける投票者装置の処理手順をコンピュータで実行するプログラムを記録した記録媒体であって、上記処理手順は以下のステップを含む：

- (a) 投票内容を集計者装置の公開鍵で暗号化して暗号化投票内容を生成し、
- (b) 乱数を発生し、
- (c) 上記暗号化投票内容を含む情報を上記乱数で攪乱して前処理文を作成し、
- (d) 上記前処理文の署名を生成し、
- (e) 上記前処理文及びその署名を選挙管理者装置へ送信し、
- (f) 上記乱数を用いて、選挙管理者装置から受信した上記前処理文に対する上記管理者のブラインド署名から上記乱数の影響を取り除いて上記暗号化投票内容を含む情報に対する上記管理者の署名を求め、
- (g) 上記暗号化投票内容を含む情報の正当性を検証し、
- (h) 上記正当性の検証に合格すると上記暗号化投票内容を含む情報と上記管理者の署名を投票データとして集計者装置へ送信し、
- (i) 上記集計者装置から受信した投票リストに自己の投票データが存在するか否かを検査する。

【請求項26】 請求項25の記録媒体において、処理手順は更に上記投票者のみが知っているタグを生成するステップと、上記暗号化投票内容と上記タグを連結して上記暗号化投票内容を含む情報を生成するステップとを含み、上記ステップ(i)は上記集計者装置から受信した上記投票リスト中の各投票データから上記タグを抽出し、そのタグが自分のものであるかを検査することにより自分の投票データが上記投票リストの中にあるかを検査するステップを含む。

【請求項27】 複数の投票者装置と、各上記投票者装置と記名通信路で接続された管理者装置と、各上記投票者装置と無記名通信路で接続された集計者装置を含む電子投票システムにおける集計者装置の処理手順をコンピュータで実行するプログラムを記録した記録媒体であって、上記処理手順は以下のステップを含む：

- (a) 各上記投票者装置から投票データとして受信した、集計者の公開鍵で暗号化された暗号化投票内容を含む情報と上記暗号化投票内容を含む情報に対する管理者の署名とを入力して上記管理者の署名を検証し、
- (b) 上記管理者署名の検証に合格すると各上記投票者装置から受信した上記投票データのリストを投票リストとして作成し、その投票リストを投票者がアクセス可能に公開し、
- (c) 上記公開鍵に対応する秘密鍵により上記暗号化内容

7
を含む情報を復号して投票者の投票内容を得、
(d) 上記復号された投票内容に基づいて候補に対する得票を集計する。

【請求項28】 請求項27の記録媒体において、上記集計者装置はそれぞれ異なる集計者により管理される、複数のシリーズ接続された分散集計者装置を有し、上記秘密鍵は上記複数の分散集計者装置に分割してそれぞれ分散秘密鍵として割り当てられており、上記ステップ(c)は各上記投票者装置から送られた上記投票データを上記シリーズの一端の分散集計者装置により受信し、それぞれの上記分散集計者装置により、割り当てられた上記分散秘密鍵を用いて上記暗号化投票内容を含む情報をシリーズに順次分散復号処理するステップを有し、最終段の上記分散集計者装置における上記分散復号処理により上記投票内容を得る。

【請求項29】 請求項27の記録媒体において、上記集計者装置はそれぞれ異なる集計者により管理される複数の分散集計者装置を有し、上記秘密鍵は上記複数の分散集計者装置に分割してそれぞれ分散秘密鍵として割り当てられており、上記ステップ(c)は各分散集計者装置により全ての上記投票者装置から上記投票データを受信し、割り当てられた上記分散秘密鍵を用いて上記暗号化投票内容を復号処理して復号中間データを生成し、それを予め決めた1つの上記分散集計者装置に送り、上記予め決めた1つの上記分散集計者装置は集められた全ての上記復号中間データを統合復号処理して上記投票内容を得るステップを有している。

【請求項30】 請求項28又は29の記録媒体において、上記ステップ(c)は上記分散集計者装置の、2以上 の予め決めた数以上が動作をすれば復号可能な閾値付分散復号処理を行う。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、電気通信システムでアンケート調査等を行う場合に、安全な無記名投票を実現しようとする電子投票システム、投票方法及びプログラム記録媒体に関する。

【0002】

【従来の技術】投票とは、有権者全員に提示された複数の候補から各投票者が予め指定された数(1又は2以上)の候補を選択し、その選択結果を集計者に与え、集計者は各候補に対する投票数を集計することである。候補としては、政治的選挙における立候補者の名前のみならず、統計調査における選択項目であってもよい。また、投票内容は、投票者が選択した候補を表す識別情報、記号、名前、項目などである。

【0003】無記名投票は、投票者と投票内容の対応を秘密にでき、個人の思想信条に関するプライバシーを守るために適しているので、電子会議やCATV等の双方向通信でのアンケート調査等に利用できる。

10 【0004】電気通信において、安全な無記名投票を行うには、投票者の偽装や二重投票、投票内容の盗聴に伴う投票内容の漏洩等の防止が必要である。これらの問題を解決する方法として、デジタル署名を用いた電子投票方式が提案されており、例えば、Atsushi Fujioka, Tatsuaki Okamoto, Kazuo Ohta: "A practical secret voting scheme for large scale elections", in Advances in Cryptology-AUSCRYPT'92, Lecture Notes in Computer Science 718, Springer-Verlag, Berlin, pp.244-251(1993)、日本国特許出願公開6-19943(1994年11月28日公開)「電子投票方法及び装置」に示されている。

【0005】この従来法では、投票者 v_i が投票内容 v_i を鍵 k_i により暗号化して暗号文 x_i とし、これにブラインド署名を得るための前処理として x_i を乱数 r_i により搅乱して前処理文 e_i を作成し、前処理文 e_i に投票者の署名 s_i を付けて選挙管理者Aに送信する。選挙管理者Aは署名 s_i に基づいて投票者 v_i の正当性を認証した後、前処理文 e_i に選挙管理者のブラインド署名 d_i を付けて投票者に返送する。投票者 v_i は前処理文 e_i に対するブラインド署名 d_i から暗号文 x_i に対する選挙管理者Aの署名 y_i を求め、これを暗号文 x_i と共に集計者Cに送信する。集計者Cは暗号文 x_i が選挙管理者Aにより署名されていることを確認して、暗号文 x_i をそのまま一覧公開する。投票者 v_i は自分の暗号文 x_i が登録されている場合は、投票内容 v_i の暗号化に使用した鍵 k_i を集計者Cに送り、登録されてない場合は集計者Cに対して異議を申し立てる。集計者Cは投票者から受信した鍵 k_i を使って暗号文 x_i から投票内容 v_i を復号し、これを集計する。

【0006】

【発明が解決しようとする課題】しかしながら、この方法では、投票者 v_i が投票締切後に公開された投票一覧から自分の暗号文 x_i が登録されたことを確認し、鍵 k_i を集計者Cに送信することが必要であり、即ち、投票者の利便性の低いシステムである。

【0007】この発明の目的は、プライバシーを侵すことなく異議申し立てが行え、また、集計者の不正や機能不全に対処できると共に、投票後に投票者が暗号化に使用した鍵を集計者に送る必要のない、簡便な電子投票システム及びその方法を提供することにある。

【0008】

【課題を解決するための手段】この発明では、投票者が投票内容を集計者の公開鍵で暗号化し、更にその暗号化投票内容を乱数で搅乱して前処理文を作成して、その前処理文に署名を付けて選挙管理者に送信する。選挙管理者は、付加された署名を用いて投票者の正当性を認証した後に、前処理文にブラインド署名して前処理文に対するブラインド署名を各投票者に送り返す。投票者は前処理文に対するブラインド署名から乱数の影響を取り除いて暗号化投票内容に対する選挙管理者の署名情報を求め、暗号化投票内容と共に投票データとして集計者に送

信する。集計者は受信した暗号化投票内容に対する署名情報が選挙管理者によって署名されていることを確認した後に、投票データを公開する。それぞれの投票者が、公開された投票データのリストに自分の暗号化投票内容が登録されていることを確認した後に、集計者は、自らが保持する秘密鍵を用いて暗号化投票内容から投票内容を取り出し、これを集計する。もし、投票リストに暗号化投票内容が登録されていない場合には、集計者に対して異議を申し立てる。また、集計者を複数とし、それぞれが復号化鍵の一部を保持し、集計者全員もしくは一定数が協力することによって、暗号化投票内容からすべての投票内容を取り出すようにしてもよい。

【0009】この発明によれば、暗号化投票内容は投票内容を乱数で攪乱しているので、選挙管理者、及び集計者は、攪乱された投票内容から投票内容を求めることが出来ず、投票の無記名性が保障できる。

【0010】ここで、復号化鍵は集計者が保持しており、投票者は、開票のために再度集計者へ通信を行なう必要がない。

【0011】集計者を複数とすれば、それらが協力することにより暗号化された投票内容を開票する場合は、異議申し立て時に、自分が正当な投票者であることは、暗号化されている投票内容と選挙管理者の署名を送るだけで示すことができる。即ち、複数存在する集計者の一部に不正者が存在したとしても、全員もしくは一定数の集計者が協力しないかぎり投票内容が明らかになることはない。

【0012】また、分散された集計者には、暗号化された投票内容が集まるので、この場合も全員もしくは一定数の集計者が協力しないかぎり、投票の間にその途中経過は明らかにならないので、公平な投票方式となっている。

【0013】更に、集計者全員でなく一定数が協力するだけで開票が可能な場合は、集計者内の何人かが不正者、もしくは、開票への協力が不可能となても、正しく開票作業を行なうことができるので、この方式は耐障害性の高いシステムであると言える。

【0014】

【発明の実施の形態】以下の実施例の説明においては、投票の例として政治的選挙における投票にこの発明を適用した場合について説明するが、前述したように、この発明の意図する投票原理は統計調査における投票にもそのまま適用できる。

第1 実施例

図1はこの発明による投票システムの全体構成を示す図である。T人の投票者 V_i ($i=1, \dots, T$) の装置（投票者装置と呼ぶ）100は、選挙管理者Aの装置（選挙管理者装置と呼ぶ）200と、また集計者Cの装置（集計者装置と呼ぶ）300と、それぞれ記名通信路400、及び無記名通信路500を介して接続されている。投票者 V_i が記名通信

路400を通して選挙管理者Aに情報を送信する場合には、その情報に送信者が誰であるかを示す送信者情報、例えば氏名 V_i 又は識別情報ID $_i$ を付加して送信するものとし、無記名通信路500を通して集計者Cに情報を送信する場合には、その情報に送信者情報を付加しないものとする。また、集計者Cは投票内容の一覧（投票リスト及び得票数リスト）を公開し、投票者は全員、これにアクセスが可能であるとする。図3に図1の投票システムにおける投票者装置100の構成例を、図4に選挙管理者装置200の構成例を、図5に集計者装置300の構成例を示し、図6にこの発明の投票システムにおける通信シーケンス例を示す。また、図2Aに選挙管理者Aが有している有権者リスト240Aを、図2Bに投票承認を与えた投票者リスト240Bを、図2Cに集計者Cが作成した投票後で、かつ集計前の投票リスト320Aを、図2Dに集計後の投票リスト320Aを、図2Eに得票数リスト320Bを例示する。

【0015】以下では、特に投票者 V_i が選挙管理者Aから投票の承認を得た後に、集計者Cに対して投票手続きする場合について説明する。

【0016】ここで、以下の説明に使用される記法をまとめて示す。

【0017】 $x = \xi_c(v, k_{pc})$: 集計者Cの暗号化関数
(x : 暗号文、 v : 投票内容、 k_{pc} : 集計者の公開鍵)
 $v = \rho_c(x, k_{sc})$: 集計者Cの復号化関数 (k_{sc} : 集計者の秘密鍵)

$s = \sigma_A(e)$: 投票者 V_i の署名作成関数 (s : 署名、 e : 暗号化投票内容)

$e = \xi_A(s)$: 投票者 V_i の署名に対する検証関数

$d = \sigma_A(d)$: 選挙管理者Aのブラインド署名作成関数
(d : ブラインド署名)

$z = \xi_A(y)$: 選挙管理者Aの署名に対する検証関数
(y : 署名、 z : 投票用紙)

$e = \omega_A(z, r)$: 攪乱関数 (r : 亂数)

$y = \delta_A(d, r)$: 亂数成分除去関数 (d : ブラインド署名)

ここで、集計者Cの暗号化関数 ξ_c と復号化関数 ρ_c は周知の公開鍵暗号方式で使用されているものであり、集計者Cは秘密鍵 k_{sc} を秘密に保持し、公開鍵 k_{pc} を投票者に公開しているものとする。また、投票者がブラインド署名を要求する際に署名対象のメッセージ m を乱数 r でブラインドする（ブラインド署名のための前処理をする）ための攪乱関数 $\omega_A(z, r)$ と、受け取ったブラインド署名 d から乱数成分 r を除去して投票用紙 z に対する選挙管理者Aの署名 y を取り出す。乱数成分除去関数 $\delta_A(d, r)$ は、選挙管理者Aが使用するブラインド署名関数 σ_A が決まれば、必然的に決まるものである。このような署名関数については、例えばR.S.A暗号の暗号化関数と復号化関数があり（Ronald Rivest, Adi Shamir, Leonard Adleman：“A method for obtaining digital sig-

natures and public-keycryptosystems", Communications of the ACM, Vol.21, No.2, pp.120-126(Feb., 1978)), ブラインド署名を要求するための前処理としての乱数による攪乱の手法についての詳細は、David Chaum : "Security without identification : Transaction systems to make big brother obsolete", Communications of the ACM, Vol.28, No.10, pp.1030-1044(Oct., 1985)に記述されている。

【0018】図3に示す投票者装置100は次のように構成されている。記憶部121には予め投票者の識別情報ID_iと名前V_iが保持されている。また、装置100内で生成されるデータのうち、後の処理に使用されるデータも記憶部121に保持される。暗号化器110は投票者V_iが選択した投票内容v_iを（ここでは例えは候補者名CND_h）集計者Cの公開鍵k_{sc}で暗号化し、暗号文x_i = ξ_c(v_i, k_{sc})を得る。タグ発生器111は乱数t_iを発生し、その乱数t_iは投票者V_iのみが知っているタグとして後述のように使用される。連結器112は暗号文x_iとタグt_iを連結してz_i = x_i || t_iを出力する。以降、z_iを投票用紙と呼ぶことにする。乱数発生器120は乱数r_iを発生する。攪乱器130はブラインド署名のための前処理として、攪乱関数e_i = ω_A(z_i, r_i)により投票用紙z_iを乱数r_iで攪乱し前処理文e_iを生成する。署名作成器140は前処理文e_iに対し投票者V_iのものであることを示すための署名s_i = σ_A(e_i, ID_i)を生成する。データ<e_i, s_i, ID_i>は送受信部190から通信路400を介して選挙管理者装置200に送信される。通信路400による選挙管理者装置200との接続は、選挙管理者装置200からブラインド署名d_iが受信されるまで維持される。

【0019】乱数成分除去器150は選挙管理者装置200から送受信部190により受信したブラインド署名d_iから乱数r_iを使って乱数成分除去関数y_i = δ_A(d_i, r_i)により乱数成分を除去し、y_iを投票用紙z_iに対する選挙管理者Aの署名として得る。署名検査部160は検証関数z_i = ξ_A(y_i)が成立するかを検査することによりy_iが正当であるか検証する。データ<z_i, y_i>は投票データとして送受信部180から集計者装置300に送信される。リスト検査部170は集計者装置300にアクセスして送受信部180により得た投票リスト320Aを検査する。

【0020】図4に示す選挙管理者装置200は有権者の識別情報ID_iが予め記録された有権者リスト240A（図2 A）と、投票の承認を与えた投票者識別情報ID_iを書き込む投票者リスト240B（図2 B）とを記録するための記憶部240と、投票者から受信した識別情報ID_iが有権者リストに載っているかを検査する投票者検査部210と、受信した投票者の前処理文e_iに対する投票者の署名s_iが正しいかを検証関数e_i = σ_A(s_i)が成立するかにより検査する署名検査部220と、正当な投票者を記憶部240の所定の領域に書き込んで投票者リストを作成する投票者リスト作成部260と、前処理文e_iに対するブラインド署名d

10

20

30

40

50

, = σ_A(e_i)を生成する署名作成器230と、投票者装置とのデータの送受信を行う送受信部250とを有している。

【0021】図5に示すように、集計者装置300は投票者装置100から受信部360により受信した投票データ<z_i, y_i>中の投票用紙z_iと選挙管理者Aの署名y_iに対し検証関数ξ_A(y_i)を使ってz_i = ξ_A(y_i)が成立するかを検査することにより署名y_iを検証する署名検査部310と、投票リスト作成部370により投票データ<z_i, y_i>に通し番号q_iを付けて投票リスト320A（図2 C）に加え、保持する記憶部320と、投票用紙z_i = x_i || t_iから暗号文x_iを分離する分離部350と、集計者の秘密鍵k_{sc}を使って復号関数ρ_Cによりx_iを復号してv_i = ρ_C(x_i, k_{sc})を投票内容として得る復号化器330と、投票内容v_iを集計する集計器340とを有する。また、記憶部320に保持されている投票リスト320Aの通し番号q_iに対応する投票データに図2 Dに示すように復号された投票内容v_iを追加する。集計結果は図2 Eに示すように各候補（CND_h; h=1, 2, ...）の得票数C_h（h=1, 2, ...）を得票リスト320Bとして記憶部320に保持される。投票リスト320Aと得票リスト320Bの内容は送受信部380を通してアクセスした投票者装置100に送信される。

【0022】以下、この第一の実施例における投票の手順を図6を参照して説明する。

ステップS1： 投票者V_iは、投票者装置100（図3）により投票の準備を以下のように行う。

【0023】ステップS1-1： 投票者V_iは、投票内容v_iを暗号化器110で集計者Cの公開鍵k_{sc}と暗号化関数ξ_Cにより暗号化し、暗号文x_i = ξ_C(v_i, k_{sc})

を作成する。更に、タグ発生器111によりタグt_iを生成し、連結器112によりx_iと連結して投票用紙

z_i = x_i || t_i

を得る。タグt_iは例えは乱数であり、投票者V_iのみが自分のものであることを知っている。

【0024】ステップS1-2： 投票者V_iは、乱数生成器120を用いて乱数r_iを生成し、攪乱器130を用いてz_iをr_iにより攪乱して前処理文

e_i = ω_A(z_i, r_i)

を作成する。

【0025】ステップS1-3： 投票者V_iは、署名作成器140を用いて、前処理文e_iと識別情報ID_iに対する署名

s_i = σ_A(e_i, ID_i)

を作成し、データ<e_i, s_i, ID_i>を送受信部190から選挙管理者装置200に送信する。

ステップS2： 選挙管理者装置200（図4）は、登録された有権者名V_iとその識別情報ID_iの関係を図2 Aに示すように有権者リスト240A（図2 A）として予め有しており、更に、投票の承認を与えた有権者の名前V_i又は識別情報ID_iを投票者リスト作成部260により書き込むための投票者リスト240B（図2 B）を有している。投票

者リストは投票受付終了後に公開されるので、承認された投票者の名前 v_i を公開してよいのであれば投票者名 v_i を書き込むが、投票者の名前が知られるのを避けるのであれば識別情報 ID_i を記録する。投票システムとしていざれか一方に決めておく。以下の説明では投票者 v_i の識別情報 ID_i を投票者リスト240B(図2B)に書き込むこととする。投票受付開始時点では、投票者リストの中には何も記録されていない。選挙管理者装置200により承認手続きを以下のように行う。

【0026】ステップS2-1：選挙管理者Aは、投票者が有権者であることを、有権者リスト240A(図2A)に識別情報 ID_i があるか否かを投票権確認部210により調べて確認する。もし無ければ、選挙管理者Aは承認を拒否する。

【0027】ステップS2-2：選挙管理者Aは、これ以前に投票者 v_i が選挙管理者Aによる承認を受けているか否かを、投票者リスト240B(図2B)に ID_i が既に書き込まれているかを投票権確認部210により調べて検査する。もし、 ID_i が既に承認されていたならば、選挙管理者Aは二重投票として承認を拒否する。

【0028】ステップS2-3： ID_i がまだ書き込まれて無ければ、選挙管理者Aは、署名検査器220を用いて、 s_i と e_i 、 ID_i が次式

$$(e_i, ID_i) = \delta_s(s_i)$$

を満足するか検査する。もし、合格ならば、選挙管理者Aは、 e_i を署名作成器230に通して、署名 d_i

$$d_i = \sigma_s(e_i)$$

を計算し、 d_i を送受信部250から投票者装置100に送信すると共に、投票者リスト作成部260により記憶部240内の投票者リスト240B(図2B)に投票者 v_i の ID_i を追加する。

【0029】ステップS2-4：投票受付終了後、選挙管理者Aは、投票者リスト240Bと投票者数を公表する。公表の方法は、予め有権者に所定の日時から一定期間内に任意の通信路を介して選挙管理者装置200の記憶部240内の投票者リスト240Bにアクセス可能であることを告知しておく。このリストへのアクセス方法は、例えば予め決めた電話番号により行うようにすることができる。投票者リスト240Bの公表場所は選挙管理者装置200内でなく、インターネット上の予め決めたアドレスに公表してもよい。

ステップS3：投票者 v_i は、投票者装置100(図3)により投票用紙とその署名情報を以下のように作成する。

【0030】ステップS3-1：投票者 v_i は、 d_i と r_i を乱数成分除去器150に入力して、投票用紙 z_i に対する署名情報 y_i

$$y_i = \delta_s(d_i, r_i)$$

を求める。

【0031】ステップS3-2：投票者 v_i は、署名検査器

$z_i = \delta_s(y_i)$ を用いて、 y_i が選挙管理者Aの署名であることを

が成立するかにより確認する。もし、不合格であったなら、投票者 v_i はデータ $\langle e_i, d_i \rangle$ を示すことにより、選挙管理者Aの不正を主張する。

【0032】ステップS3-3：投票者 v_i は、前記署名確認が合格であれば送受信部180からデータ $\langle z_i, y_i \rangle$ を集計者装置300に通信路500を通して送信する。

ステップS4：集計者Cは、集計者装置300により以下のようにして票を収集する。

【0033】ステップS4-1：集計者Cは、投票者から受信部360により投票データ $\langle z_i, y_i \rangle$ を受信し、署名検査器310を用いて y_i が投票用紙 z_i に対する正当な署名であることを

$$z_i = \delta_s(y_i)$$

が成立するかを検査することにより確認する。もし、合格ならば、投票リスト作成部370により投票リスト230A(図2C)に、それぞれの投票用紙 z_i とその署名 y_i に一連の番号 q により番号付けをし、投票データ $\langle q, z_i, y_i \rangle$ として掲載する。

【0034】ステップS4-2：すべての投票後、集計者Cは送受信部380を通して記憶部320にアクセス可能とすることにより投票リスト320Aを公表する。この投票リストはすべての投票者からアクセスが可能であるとする。公表方法は前述の投票者リスト240Bの場合と同様に、公表期間、公表場所、を予め告知しておく。ステップS5：投票者 v_i は、投票者装置100により以下のようにして検証を行う。

【0035】ステップS5-1：投票者 v_i は、送受信部180により集計者装置300の記憶部320をアクセスし、投票リスト320Aの内容を受信し、投票リスト320Aに掲載された投票の数がStep 2-4で公表された投票者の数と一致するかを表検査器170で検査する。もし、不合格ならば、番号 q と乱数 r_i を公表して、選挙管理者Aの不正を主張する。

【0036】ステップS5-2：投票者 v_i は、自らの投票用紙 z_i が、投票リスト320Aに掲載されているかを表検査器170で検査する。その検査として、 z_i そのものがリスト中にあるかを検査してもよいし、 $z_i = x_i \| t_i$ 中のタグ t_i が自分のものであるか検査してもよい。もし、掲載されていなければ、投票データ $\langle z_i, y_i \rangle$ を示して、集計者Cの不正を主張する。

ステップS6：集計者Cは、集計者装置300により以下のようにして開票、及び、集計を行う。

【0037】ステップS6-1：受信部360により投票者 v_i からの投票用紙 z_i と署名 y_i の受信開始後、前記不正の通知が所定時間内になければ、集計者Cは、分離部350で投票用紙 $z_i = x_i \| t_i$ から x_i を分離し、復号化器330にて開票し、秘密鍵 k_{sc} を使って投票内容 v_i を

により求め、投票内容 v_i が正しい投票か、つまり投票内容 v_i が予め提示した候補を表す名前又は記号となるかを検査する。なっていなければ無効投票とされる。

【0038】ステップ S6-2：集計者 C_i は、図 2 C の投票リストの投票内容 v_i を集計器 340 を用いて集計し、各候補に対する投票数を得て、その結果を図 2 E に示す得票数リスト 320B として公表するとともに、q 番目の投票データ $\langle x_i, t_i, v_i \rangle$ に対し図 2 D に示すように、 v_i を追加する。集計結果は投票リスト 320A に添付して公表する。

ステップ S7：投票者 V_i は、投票者装置 100 により集計者 C_i の操作が正しいことを確認する。つまり図 2 C に示す投票リスト 320A 中にすべての v_i が追加されたか、また投票者 V_i の x_i と v_i とが対応しているかを確認する。

【0039】なお、上記ステップ S5 は省略してもよい。更に、ステップ S6-2における得票数リストの公表、及びステップ S7 も省略してよい。

【0040】前述の実施例では投票者 V_i が集計者 C_i の暗号化関数 ξ_c を使って投票内容 v_i を $x_i = \xi_c(v_i, k_{pc})$ と暗号化し、集計者 C_i に投票データ $\langle x_i, v_i \rangle$ を送るので、集計者 C_i は、もしそのつもりになれば Step 4-2 で投票リストを公開する前であっても集計者の秘密鍵 k_{pc} を使って x_i 中の x_i を復号関数 $v_i = \rho_c(x_i, k_{sc})$ により復号して v_i を得ることができる。即ち、投票リストの公開を待たずして投票の傾向、途中結果などの情報を得て、その情報を公式の集計結果が出る前に特定な人に漏らすことができるので、選挙の公平性の点から好ましくない。また、第 1 実施例では、集計者装置 300 が故障した場合、投票の集計をスケジュール通りに完了できないこともある。以下では複数の集計者によりそれぞれ管理される複数の集計者装置により暗号化投票内容を復号し、集計することによりこれらの点について改善した実施例を説明する。

【0041】ここで、分散集計者の暗号関数(暗号化関数 ξ_c 、復号化関数 ρ_c)は、公開鍵暗号方式で使用されるものであるが、各暗号文 x_i に対し全ての分散集計者がそれぞれもっている分散秘密鍵 k_{scj} で復号処理を行なうことではじめて、暗号文が復号可能となったり、又は復号処理に必要な人数にしきい値 U_i ($2 \leq U_i \leq U$) が存在し、一定数のしきい値付分散集計者が集まれば復号可能なようなものとする。このような暗号関数については、例えば ElGamal 暗号 (Taher ElGamal : "A public keycrypto system and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, Vol. IT-31, No. 4, pp. 469-472 (July, 1985)) の暗号化関数と復号化関数があり、これの分散した復号者による復号の手法やしきい値を導入した手法についての詳細は、Yvo Desmedt, Yale Frankel : "Threshold cryptosystems" in Advances in Cryptology-CRYPTO'89, Lecture Notes in Computer Science 435, Springer-Verlag, Berlin, pp. 307-315 (1990) に記述されている。

第2実施例

図 7 は第 2 実施例による投票システムの全体の構成を示す。この実施例では、それぞれの投票者装置 100 が通信路 400 を介して選挙管理人装置 200 に接続され、また通信路 500 を通して 1 つの集計者装置に接続される点は第 1 実施例と同じであるが、構成上の異なる点は、複数の集計者装置 300_j ($j = 1, \dots, U$ 、以下分散集計者装置と呼ぶ) を設け、分散集計者装置 300_j は全ての投票者からの暗号文 x_i を復号処理して $x_{i,j}$ を生成し、次の分散集計者装置 300_{j+1} に送り、同様に j 番目の分散集計者装置 300_j は直前の分散集計者装置 300_{j-1} から受けた復号処理データ $x_{i,j-1}$ を復号処理して $x_{i,j}$ を生成し、次の分散集計者装置 300_{j+1} に送る。最後の分散集計者装置 300_U による復号処理により初めて投票内容 v_i が得られる。第 1 実施例と同様に、通信路 400 を通して投票者装置 100_i がデータを管理者装置 200 に送る場合は、投票者 V_i の識別情報 ID_i を付けて送るが、通信路 500 を通してデータを分散集計者装置 300_j に送る場合は、識別情報 ID_i を付けない。

【0042】通信シーケンス例や各投票者装置 100_i の構成例、選挙管理者装置 200 の構成例などは集計者装置 300 を分散集計者装置 300_j とする以外は先と同様である。また、各投票者は共通の公開鍵 k_{pc} を使って投票内容 v_i を $x_i = C(v_i, k_{pc})$ により暗号化する点も第 1 実施例と同じであるが、集計者 C₁ ~ C_U は秘密鍵 k_{sc} から生成された U 個の分散秘密鍵 $k_{sc1}, k_{sc2}, \dots, k_{scU}$ をそれぞれ有しており、それを使って復号処理を行うが、各集計者装置 300_j 単独では暗号文 x_i から投票内容 v_i を復号できない。暗号システムとして前述の ElGamal 暗号を使用する場合は、このような分散秘密鍵 $k_{sc1}, k_{sc2}, \dots, k_{scU}$ を、例えばこれらの鍵の値の総和が公開鍵 k_{pc} に対応する秘密鍵 k_{sc} の値と等しくなるように決めることができることが前述の Desmedt-Frankel の文献に示されている。

【0043】図 8 A は投票者装置 100_i ~ 100_U からの投票を集票する第 1 分散集計者装置 300₁ の構成を示し、署名検査部 310 と、記憶部 320 と、集計器 340 と、分離部 350 と、分散復号処理部 331 と、受信部 360 と、投票リスト作成部 370 と、送受信部 380 とを有している。図 5 に示した第 1 実施例の集計者装置 300 とは次の点で異なっている。第 1 に、分散復号処理部 331 において暗号文 x_i に対し分散秘密鍵 k_{sc1} を使って復号処理 $x_{i,1} = \rho_{c1}(x_i, k_{sc1})$ により復号中間データ $x_{i,1}$ を生成し、それを次の分散集計者装置 300₂ に送ることである。第 2 に、集計器は最後の分散集計者装置 300_U から復号投票内容 v_i を受信し、それを集計することである。第 2 ~ 第 U 分散集計者装置 300₂ ~ 300_U のそれぞれは第 j 分散集計者装置 ($2 \leq j \leq U$) を代表して図 8 B に示すように、分散復号処理部 331 を有するだけであり、前段の分散集計者装置 300_{j-1} から受信した復号中間データ $x_{i,j-1}$ に対し、分散秘密鍵 k_{scj} を使って復号処理 $x_{i,j} = \rho_{cj}(x_{i,j-1}, k_{scj})$ により復号中間データ $x_{i,j}$ を生成し、それを次段の分散集計者装

置 $300_{1..1}$ に送信する。ただし、最終段の分散集計者装置 300_u では復号処理 $x_{1u} = \rho_{cu}(x_{1u-1}, k_{scu})$ により x_{1u} を最終的復号結果である投票内容 $v_i = x_{1u}$ として得ることができ、その投票内容 v_i を第1分散集計者装置 300_1 に送信する。

【0044】この第2実施例における投票の手順を示す。この実施例においても、第1実施例におけるステップS1からステップS5までの手順と同じ手順が実行される。ただし、各投票者装置 100_i から投票データ $\langle z_i, v_i \rangle$ を受けるのは第1分散集計者装置 300_1 であるものとする。この第2実施例は第1実施例のステップS6, S7を以下のように変更したものであり、Uは分散集計者装置の数である。

ステップS6： 分散集計者 C_j ($j=1, \dots, U$) は、分散集計者装置 300_1 により、以下のようにして集計を行う。

【0045】ステップS6-1： 第1分散集計者装置 300_1 は、各投票者装置 100_i ($i=1, \dots, T$)からの投票データ $\langle z_i, v_i \rangle$ 中の $z_i = x_i \| t_i$ を分離部350で暗号文 x_i とタグ t_i に分離し、分散秘密鍵 k_{sc1} を使って分散復号処理部330により次の復号処理

$$x_{11} = \rho_{c1}(x_i, k_{sc1})$$

を行い、復号中間データ x_{11} を得て、これを次の第2分散集計者装置 300_2 に送る。

【0046】以下同様に、第j分散集計者装置 300_j は第j-1分散集計者装置 300_{j-1} からの復号中間データ x_{1j-1} に対し、分散秘密鍵 k_{scj} を使って分散復号処理部330により復号処理

$$x_{1j} = \rho_{cj}(x_{1j-1}, k_{scj})$$

を行い、得られた復号中間データ x_{1j} を次の第j+1分散集計者装置 300_{j+1} に送る。

【0047】最後の第U分散集計者装置 300_u は、第U-1分散集計者装置からの復号中間データ x_{1u-1} に対し分散秘密鍵 k_{scu} を使って分散復号処理部330により復号処理

$$v_i = x_{1u} = \rho_{cu}(x_{1u-1}, k_{scu})$$

を行うことにより投票内容 v_i を得る。第U分散集計者装置 300_u は得られた投票内容が無効でないか検査する。

【0048】ステップS6-2： 第U分散集計者 C_u は、投票内容 v_i を集計器340を用いて集計し、その結果を公表するとともに、投票内容 v_i を投票リストに追加する。

Step 7： 投票者 V_i は、投票者装置 100_i により第U分散集計者装置 300_u の操作が正しいことを確認する。

【0049】この様に、第2実施例では復号処理を複数の分散集計者装置 $300_1 \sim 300_u$ により順次行い、最後の分散集計者装置 300_u において投票内容 v_i が得られるので、どの分散集計者も集計開始前に単独で開票して v_i を得ることはできない。

第3実施例

図9は第3実施例における投票システム全体構成を示す。この実施例では、各投票者装置 100_i ($i=1, \dots, T$)は全ての分散集計者装置 $300_1 \sim 300_u$ に通信路500を通して接

続可能とされており、生成した投票データ $\langle z_i, v_i \rangle$ を全ての分散集計者装置 $300_1 \sim 300_u$ に送信する。各投票者装置 100_i 及び選挙管理者装置200の構成は第1及び第2実施例の場合と同じである。

【0050】第1～第U-1分散集計者装置 $300_1 \sim 300_{U-1}$ の構成は第j分散集計者装置 300_j で代表して図10Aに示すように、各投票者装置 100_i から受信した投票データ $\langle z_i, v_i \rangle$ の z_i に対する署名 y_i の検証を行う署名検査部310と、 z_i から暗号文 x_i を分離する分離部350と、暗号文に対し、分散秘密鍵 k_{scj} を使って復号処理 $x_{1j} = \rho_{cj}(x_i, k_{scj})$ により復号中間データ x_{1j} を生成する分散復号処理部331とを有し、復号中間データ x_{1j} を予め決めた1つの分散集計者装置、この例では 300_j に送信する。分散集計者装置 300_j は図10Bに示すように、図10Aの構成に更に記憶部320と、統合復号部332と、集計器340と、前分散集計者装置 $300_1, \dots, 300_{j-1}$ から集めた投票データ $\langle z_i, v_i \rangle$ にそれぞれ通し番号qを付けて投票リスト320Aに書き込む投票リスト作成部370と、投票リスト320Aと得票数リスト320Bをアクセス可能とするため投票者装置 100_i と送受信を行う送受信部380とが追加された構成となっている。記憶部331には受信した投票データのリストを掲載する投票リスト320Aと、集計結果を表す各候補の得票リスト320Bが形成される。統合復号部332はそれぞれの分散集計者装置 $300_1 \sim 300_j$ で生成された復号中間データ $x_{11} \sim x_{1j}$ に対し復号関数 ρ_c により復号処理 $v_i = \rho_c(x_{11}, \dots, x_{1j})$ を行い投票内容 v_i を得て、集計器340に与える。集計器340は投票内容 v_i の有効性を検査し、有効であれば記憶部320内に作成した得票リストの対応する候補の得票数に1を加算する。また投票リストの対応する投票データに v_i を追加する。

【0051】この第3実施例においても、各分散集計者装置は単独で暗号文 x_i から投票内容 v_i を復号することはできないので、選挙の公平性が保証される。

変形実施例1

第2及び第3実施例では、全員の分散集計者 $C_1 \sim C_U$ が協力しなければ暗号文 x_i から投票内容 v_i を復号できない。しかしながら、例えば前述のDesmedt-Frankelの方法に従って分散復号処理部331を構成することにより、少なくとも1個 ($2 \leq L \leq U-1$) の分散集計者装置があれば、公開鍵 k_c により暗号化された暗号文 x_i から v_i を復号可能である。この方法を第2実施例(図7, 8A, 8B)に適用した実施例を説明する。

【0052】例えば分散集計者装置 $300_1 \sim 300_u$ のいずれか1つ、例えば 300_1 が故障しても、その直前の分散集計者装置 300_{U-1} は分散集計者装置 300_u を迂回して分散集計者装置 300_{U-1} に復号中間データ x_{1U-1} を送る。分散集計者装置 300_{U-1} は復号中間データ x_{1U-1} に対し分散秘密鍵 k_{scU-1} を使って $x_{1U-1} = \rho_c(x_i, k_{scU-1})$ により中間復号データ x_{1U-1} を得て、それを更に次段の分散集計者装置 300_u に渡せばよい。この場合に使用される分散秘密鍵

の生成方法は、例えば前述のDesmedt-Frankelの文献に示されている。また、全ての分散集計者装置 $300_1 \sim 300_v$ の構成を図8Aに示す構成とすれば、第1分散集計者装置 300_1 が故障しても、それに代わって次の段の分散集計者装置 300_i が投票者装置 $100_1 \sim 100_v$ から投票データ $\langle z_1, v_1 \rangle$ を受信し、分散集計者装置 300_i の機能を代行することができる。最終段の分散集計者装置 300_v は復号処理により得られた投票内容 v_i を、代行の分散集計者装置 300_i に送信すればよい。この実施例によれば、U-L以下のいずれかの分散集計者装置が故障しても、投票の集計を行うことができる。

変形実施例2

同様に、第3実施例(図9、10A、10B)においても、分散復号処理部331と統合復号部332にDesmedt-Frankelの方法を適用すれば、分散集計者装置 $300_1 \sim 300_{v-1}$ のうち少なくともL個($2 \leq L \leq U-1$)以上の分散集計者装置による復号中間データが得られるならば v_i を復号することができる。例えば分散集計者装置 $300_1 \sim 300_{v-1}$ が故障した場合、残りの分散集計者装置 $300_{v-1+1} \sim 300_v$ からの復号中間データ $x_{1,0-1,1} \sim x_{1,v}$ を分散集計者装置 300_v の統合復号部332に与え、それらに対する復号処理 $v_i = \rho_c(x_{1,0-1,1}, x_{1,0-1,2}, \dots, x_{1,v})$ により投票内容 v_i を復号できる。得られた投票内容 v_i は集計器340により有効性が検査され、有効であれば記憶部320内の得票リストの v_i に対応する候補の得票に1を加算する。

【0053】この変形実施例において、全ての分散集計者装置 $300_1 \sim 300_v$ の構成を図10Bに示すものと同じに構成すれば、U-L個以内のどの分散集計者装置が故障しても、残りの1つに対し図10Bの分散集計者装置と同様の動作をさせることにより投票の集計を行うことができる。

【0054】図3～5、8A、8B、10A、10Bに示す各装置はその機能構成を示したものであり、これら各機能を動作を順次行わせるための制御部を備え、また全体乃至一部をコンピュータにより実行させることもできる。

【0055】

【発明の効果】以上に説明したように、この発明では、投票内容 v_i を集計者の公開暗号鍵KPCで暗号化しているので、投票者は投票内容を復号化するために、鍵を集計者に送信する必要がない。

【0056】集計者を複数とした場合には、集計者全員の合意が得られなければ開票作業が開始されない。

【0057】更に、一定数の集計者が開票できる場合には、正当な集計者がある程度集まれば開票作業が開始でき、不正者もしくは故障者の影響を除去できる。

【0058】また、集計者が投票内容を改竄(かいざん)しても、公開された投票内容の一覧表を閲覧することで、投票内容の改竄を検出できる。即ち、自らの投票が利用されていないときには、暗号化された投票用紙 z_i と選挙管理者の署名 y_i を公開し、不正を主張すればよい。この際、不正な集計者の数が一定であるならば異議申し立て時のプライバシーは保証されている。

【0059】更に、複数の集計者をおいた場合に、この発明では、暗号化鍵を用いて、投票内容を暗号化して送信しているので、投票用紙の収集の際に、集計者が途中経過を漏洩して選挙に影響を及ぼすといった不正が防止できる。

【0060】以上より、この発明では集計者の暗号化鍵を用いて、投票者の利便性を向上させ、また、集計者を複数とすることにより、途中経過を漏洩して選挙に影響を及ぼすといった不正を解決できる。

【図面の簡単な説明】

【図1】この発明の第1実施例による投票システムの全体構成を示すブロック図。

【図2】Aは有権者リストを示す表、Bは投票者リストを示す表、Cは投票リストを示す表、Dは投票リストを示す表、Eは得票数リスト。

【図3】投票者装置100の機能構成例を示すブロック図。

【図4】選挙管理者装置300の機能構成例を示すブロック図。

【図5】集計者装置400の機能構成例を示すブロック図。

【図6】投票処理手順を示す図。

【図7】第2実施例による投票システムの全体構成を示すブロック図。

【図8】Aは図7における分散集計者装置 300_i の機能構成例を示すブロック図、Bは図7における分散集計者装置 $300_{v-1} \sim 300_v$ の機能構成を示すブロック図。

【図9】第3実施例による投票システムの全体構成を示すブロック図。

【図10】Aは図9における分散集計者装置 $300_1 \sim 300_{v-1}$ の機能構成を示すブロック図、Bは図9における分散集計者装置 300_v の機能構成を示すブロック図。

【図1】

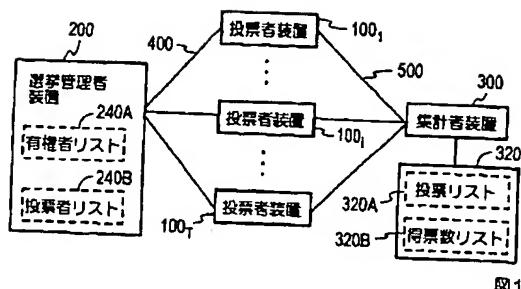


図1

【図2】

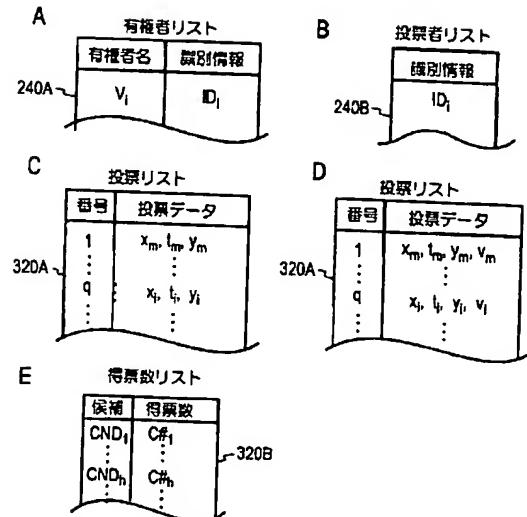


図2

【図3】

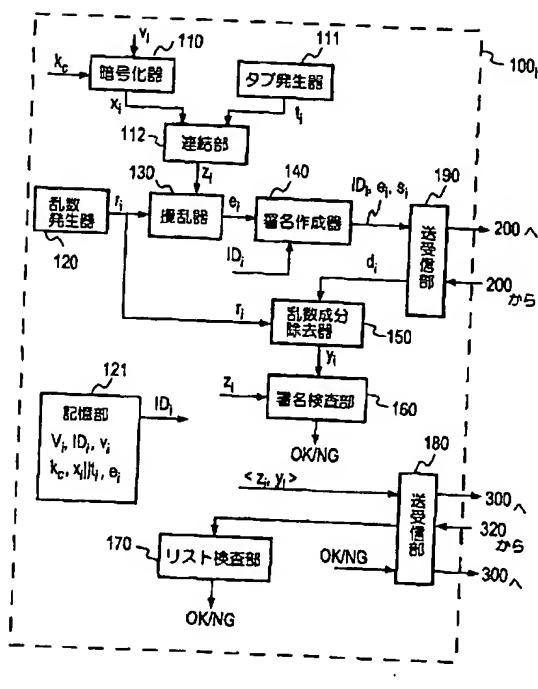


図3

【図4】

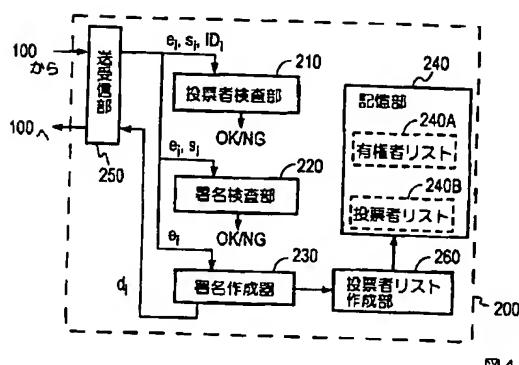


図4

【図5】

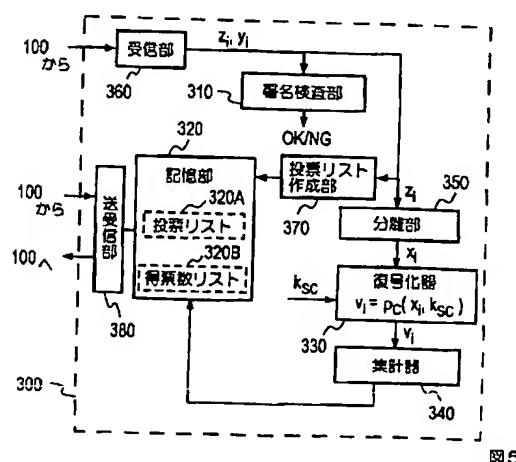


図5

【図6】

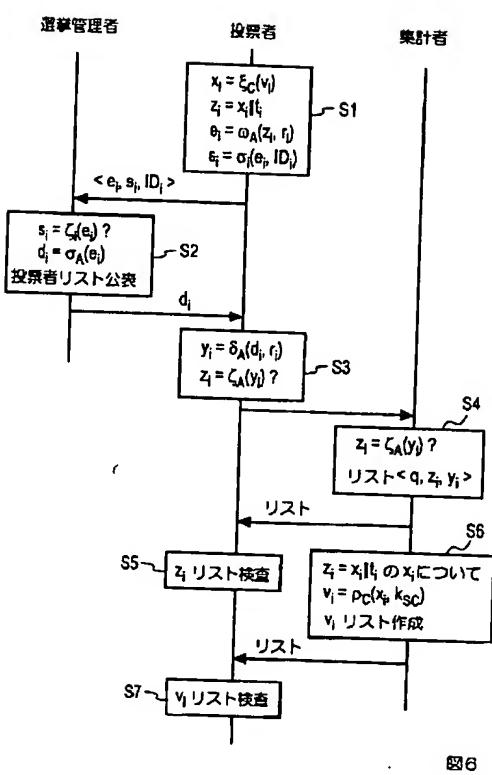


図6

【図7】

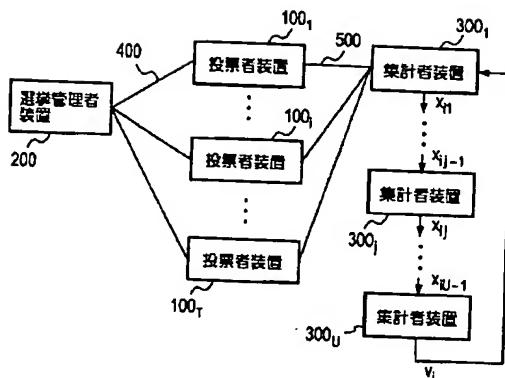


図7

【図8】

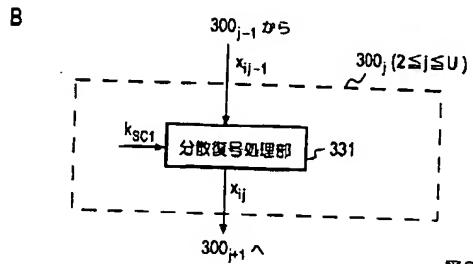
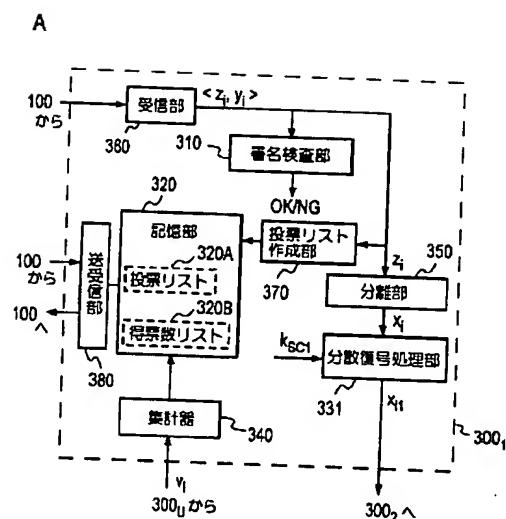


図8

【図9】

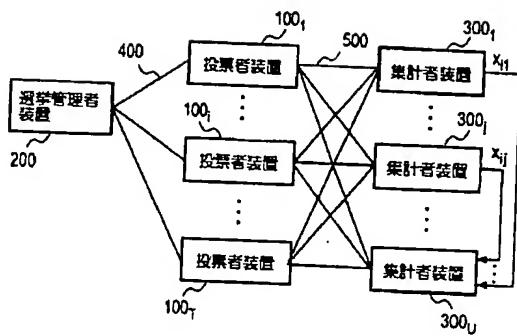
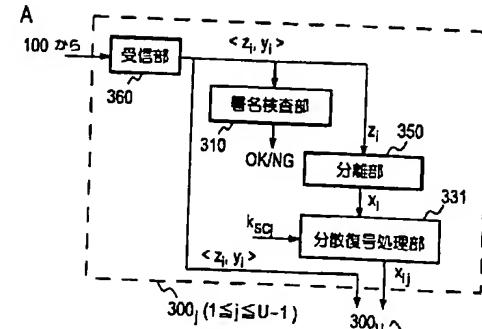


図9

【図10】



A

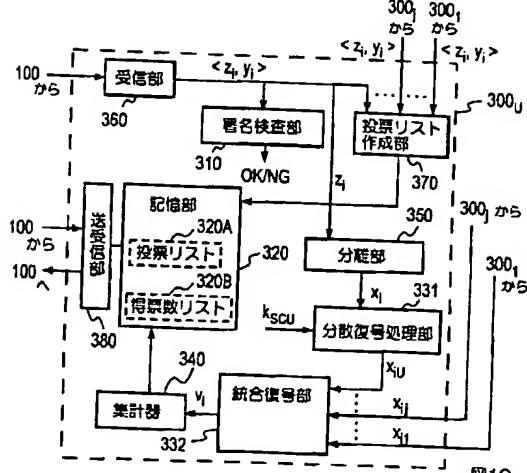


図10

【手続補正書】

【提出日】平成11年11月22日(1999.11.22)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】請求項7

【補正方法】変更

【補正内容】

【請求項7】 請求項1又は2の電子投票方法において、上記ステップ(a)は上記前処理文に対する投票者の署名を生成し、上記前処理文と共に上記管理者装置に送信するステップを含み、上記ステップ(b)は上記前処理文に対する上記投票者の署名の正当性を検査するステップを含む。

(19) Japan Patent Office (JP)
 (12) Japanese Unexamined Patent Application Publication (A)

(11) Japanese Unexamined Patent
 Application Publication Number

2000-207483
 (P2000-207483A)

(43) Publication date 28 July 2000 (2000.7.28)

(51) Int. Cl. ⁷	Identifying symbols	FI	Subject codes (reference)
G 06 F 19/00		G 06 F 15/28	B
G 09 C 1/00	640	G 09 C 1/00	640B
H 04 L 9/32		H 04 L 9/00	675D

Request for examination: Filed Number of Claims: 30 OL (14 pages total)

(21) Application No.	H11-310468	(71) Applicant	000004226 Nippon Telegraph and Telephone Corp. 3-1 Otemachi 2-chome, Chiyoda-ku, Tokyo
(22) Filing date	1 November 1999 (1999.11.1)	(72) Inventor	Fujioka, Atsushi c/o Nippon Telegraph and Telephone Corp. 3-1 Otemachi 2-chome, Chiyoda-ku, Tokyo
(31) Priority Claim No.	Patent Application H10-320173	(72) Inventor	Abe, Masayuki c/o Nippon Telegraph and Telephone Corp. 3-1 Otemachi 2-chome, Chiyoda-ku, Tokyo
(32) Priority date	11 November 1998 (1998.11.11)	(72) Inventor	Miura, Fumimitsu c/o Nippon Telegraph and Telephone Corp. 3-1 Otemachi 2-chome, Chiyoda-ku, Tokyo
(33) Priority country	Japan (JP)	(74) Agent	100066153 Patent Attorney Kusano, Takashi (and 1 other)

(54) {Title of invention} Electronic voting method, voting system and program recording medium

(57) {Abstract}

{Problem} To eliminate the need for a voter to send the key used to encrypt the content of the vote to a counter.

{Solution} A voter V_i encrypts the vote content v_i with the public key k_{PC} of a counter C, associates a tag t_i with the encrypted vote content x_i to obtain z_i , randomizes z_i using a random number r_i to create a preprocessed text e_i , and sends a signature s_i for that preprocessed text and the preprocessed text e_i to an election administrator A. The election administrator A creates a blind signature d_i for the preprocessed text e_i and returns it to the voter V_i . From the blind signature d_i , the voter obtains the election administrator's signature information y_i with the effect of the random number r_i eliminated therefrom, and sends the vote data $\langle z_i, y_i \rangle$ to the counter C. The counter C verifies the election administrator's signature y_i , and verification is successful, creates a vote list containing the data $\langle z_i, y_i \rangle$ and discloses it to the voters. The voter V_i verifies the vote list and confirms that data $\langle z_i, y_i \rangle$ matching his own tag t_i is present in the list. The counter C decrypts the x_i in z_i to obtain the vote content v_i , and counts up the number votes for the candidates.

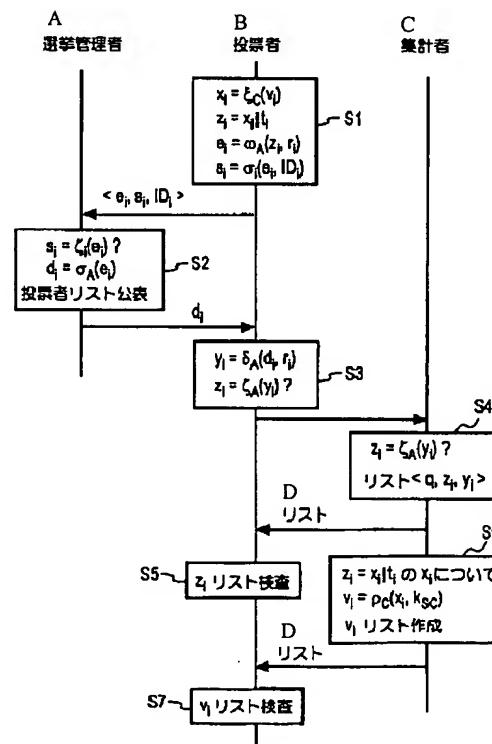


Figure 6

S2: Voter list publication

S4: List $\langle q, z_i, y_i \rangle$

S5: z_i list verification

S6: For x_i of $z_i = x_i || t_i$

$v_i = p_C(x_i, k_{sc})$

v_i list generation

S7: v_i list verification

A: Election administrator

B: Voter

C: Counter

D: List

{Scope of patent Claims}

{Claim 1} An electronic voting method whereby voters obtain approval for a vote from an administrator and then send vote data to a counter device and the counter device counts the votes, comprising the following steps:

(a) each voter encrypts the content of his vote for selected candidates by means of an encryption device using the public key of the counter device, randomizes information containing the encrypted voted content with a random number to generate a preprocessed text, and sends that text to the administrator device;

(b) said administrator device confirms the legitimacy of each voter device,

inputs the received preprocessed text into a signature generating device to generate a blind signature for the preprocessed text and returns it to the voter device;

(c) each voter removes the effect of said random number component from the blind signature for the preprocessed text, determines the administrator signature of said administrator for said information containing encrypted vote content, and transmits that administrator signature and said information containing encrypted vote content as vote data to the counter device;

(d) said counter decrypts said information containing encrypted vote content by means of a decryption device using a secret key corresponding to said public key to obtain the vote content, and counts up the votes for candidates corresponding to said vote content.

{Claim 2} An electronic voting method as per Claim 1, which further comprises, prior to aforementioned step (d), a step (d-0) whereby the counter inputs the received aforesaid encrypted vote content and said signature information into a signature verification device to verify that the preprocessed text has been signed by said administrator, and publishes a list of information containing encrypted vote content, and a step (d-1) whereby said voter confirms that his own encrypted vote content is present in the list.

{Claim 3} An electronic voting method as per Claim 1 or 2, wherein the step (a) of randomizing said information containing encrypted vote content comprises the step of generating a tag known only to said voter and the step of associating said tag with said encrypted vote content to randomize it using said random number; and wherein said step (d-1) comprises the step of separating said tag from the vote data in said list and verifying whether the tag is one's own.

{Claim 4} An electronic voting method as per Claim 1 or 2, wherein said step (b) comprises the step of publishing a list of information representing voters who were given said blind signature as a voter list, and wherein said step (c) comprises the step of confirming that information representing oneself is contained in said voter list.

{Claim 5} An electronic voting method as per Claim 1 or 2, wherein said step (d) comprises the step of publishing the results of counting said vote content.

{Claim 6} An electronic voting method as per Claim 1 or 2, wherein, in said step (a), said voter appends voter identification information to said preprocessed text and transmits it to said administrator device; in step (b), said administrator confirms said voter based on said voter identification information; and in step (c), said voter transmits said vote data anonymously to said

counter device.

{Claim 7} An electronic voting method as per Claim 1 or 2, wherein said step (a) comprises the step of generating a voter signature for said vote and transmitting it together with said vote to said administrator device, and wherein said step (b) comprises the step of verifying the authenticity of said voter signature for said vote.

{Claim 8} An electronic voting method as per Claim 1, wherein: said counter device comprises multiple distributed counter devices connected in series, with each distributed counter device being administered by a different counter; said secret key is split up among said multiple distributed counter devices and assigned as a distributed secret key to each of them; in said step (c), each voter transmits said vote data to a distributed counter device at one end of said series; and said step (d) comprises the step whereby said counter devices in series successively perform decryption processing of said information containing encrypted vote content by means of a decryption unit with which each of them is provided, using said distributed secret key, and obtain said vote content by means of the final stage decryption processing.

{Claim 9} An electronic voting method as per Claim 1, wherein said counter device comprises multiple distributed counter devices, with each distributed counter device being administered by a different counter; said secret key is split up among said multiple distributed counter devices and assigned as a distributed secret key to each of them; in said step (c), each voter transmits said vote data to all said distributed counter devices; and said step (d) comprises the step whereby said counter devices separately perform decryption processing of said encrypted vote content by means of a decryption unit with which each of them is provided, using said distributed secret key, generating intermediate decrypted data, gathering it at one predetermined distributed counter device, and performing decryption processing to obtain said vote content.

{Claim 10} An electronic voting method as per Claim 8 and 9, wherein said decryption processing is thresholded decryption processing whereby decryption is possible when at least a predetermined number of two or more of said distributed counter devices is operating.

{Claim 11} An electronic voting system with multiple voter devices, an administrator device connected to each of said voter devices via a named communication channel, and {sic} connected to each of said voter devices via an anonymous communication channel, wherein each said voter device comprises:

an encryption device which encrypts the vote content with the public key of the counter device to generate encrypted vote content;

a random number generating device which generates random numbers;

a randomizing device which randomizes said encrypted vote content with an aforesaid random number to create preprocessed text;

a means which transmits said preprocessed text to said administrator device;

a random number component removing device which removes the effect of said random number from said administrator device's blind signature for said preprocessed text received from said administrator device to find the administrator signature of

said administrator device for said information containing encrypted vote content; and a means which transmits said administrator signature and said information containing encrypted vote content to the counter device as vote data; said administrator device comprises:

a blind signature generating device which generates a blind signature for said preprocessed text received; and a means which transmits said blind signature to voter devices; and said counter device comprises:

a decryption device which decrypts said information containing encrypted vote content in said vote data by means of a secret key corresponding to said public key to obtain said vote content; and

a counting device which counts up the votes for candidates based on said decrypted vote content.

{Claim 12} An electronic voting system as per Claim 11, wherein said voter device additionally comprises an administrator signature verification device which verifies said administrator signature for said information containing encrypted vote content, and if the verification by the administrator signature verification device is successful, transmits said vote data to said counter device, and wherein said counter device comprises an administrator signature verification device which accepts as input said administrator signature and said information containing encrypted vote content in said vote data received from said voter device to verify said administrator signature.

{Claim 13} An electronic voting system as per Claim 11, wherein said voter device additionally comprises a voter signature generating device which generates a voter signature for said preprocessed text and transmits its to said administrator device, and said administrator device comprises a voter signature verification device which verifies said preprocessed text received from each voter device and the voter signature thereof, and if that verification succeeds, generates said blind signature by means of said blind signature generating device.

{Claim 14} An electronic voting system as per Claim 11, wherein said counter device comprises a vote list generating device which, if verification of said administrator signature is successful, generates a list of said vote data received from each said voter device as a vote list, and publishes it to make it accessible to said voter, and wherein said voter device comprises a vote list verification device which verifies whether or not one's own encrypted vote content is present in the vote list received from said counter device.

{Claim 15} An electronic voting system as per Claim 14, wherein said voter device comprises a tag generating device which generates a tag known only to said voter, an associating device which associates said encrypted vote content and said tag to generate said information containing encrypted vote content, and a list verification unit which extracts said tag from each vote datum in said vote list and examines whether on not that tag is one's own in order to verify whether one's own vote data is contained in said vote list.

{Claim 16} An electronic voting system as per Claim 11, wherein said counter device comprises multiple distributed counter devices connected in series, each administered by a different counter; said secret key is split up among said multiple distributed counter devices and assigned as a distributed secret

key to each of them; each said voter device transmits said vote data to a distributed counter device at one end of said series; and said distributed counter devices comprise decryption processing units which in series successively perform decryption processing of said information containing encrypted vote content using said distributed secret key which is assigned to each other them, and obtain said vote content by means of decryption processing by said decryption processing unit of said distributed counter device which is at the final stage.

{Claim 17} An electronic voting system as per Claim 11, wherein said counter device comprises multiple distributed counter devices connected in series, each administered by a different counter; said secret key is split up among said multiple distributed counter devices and assigned as a distributed secret key to each of them; each said voter device transmits said vote data to all said distributed counter devices; said distributed counter devices each comprises a decryption processing unit, each of which separately performs decryption processing of said encrypted vote content using said distributed secret key, which is assigned to each of them, to generate intermediate decrypted data, and sends it to a predetermined one said distributed counter device; and said predetermined one said distributed counter device comprises a combination decryption unit which performs decryption processing of all gathered said intermediate decrypted data to obtain said vote content.

{Claim 18} An electronic voting system as per Claim 16 or 17, wherein said decryption processing unit performs thresholded decryption processing whereby decryption is possible when at least a predetermined number of two or more of said distributed counter devices is operating.

{Claim 19} In an electronic voting system which comprises multiple voter devices, an administrator device connected to each of said voter devices via a named communication channel, and a counter device connected to each of said voter devices via an anonymous communication channel, a voter device comprising:

an encryption device which encrypts the vote content with the public key of the counter device to generate encrypted vote content;

a random number generating device which generates random numbers;

a randomizing device which randomizes information containing said encrypted vote content with an aforesaid random number to create preprocessed text;

a voter signature generating device which generates a voter signature for said preprocessed text;

a means which transmits said preprocessed text and its voter signature to the administrator device;

a random number component removing device which accepts as input said random number and the administrator's blind signature for said preprocessed text received from said administrator device and removes the effect of said random number from said blind signature to find said administrator's signature for said information containing encrypted vote content;

a signature verification device which accepts as input said administrator signature for said encrypted vote content and said information containing encrypted vote content and verifies said administrator signature;

a means which transmits said administrator signature and said

information containing encrypted vote content to the counter device as vote data if the signature is successfully verified by the signature verification device; and
a list verification device which verifies whether or not one's own vote data is present in the vote list received from said counter device.

{Claim 20} A voter device as per Claim 19 which additionally comprises a tag generating device which generates a tag known only to said voter, and an associating device which associates said encrypted vote content with said tag to generate said information containing encrypted vote content, wherein said list verification part extracts said tag from each vote datum in said vote list received from said counter device and examines if that tag is one's own to verify that one's own vote data is present in said vote list.

{Claim 21} In an electronic voting system which comprises multiple voter devices, an administrator device connected to each of said voter devices via a named communication channel, and a counter device connected to each of said voter devices via an anonymous communication channel, a counter device comprising:

an administrator signature verification device which accepts as input information containing encrypted vote content encrypted with the public key of the counter and the administrator's signature for said information containing encrypted vote content, which are received as vote data from each said voter device, and verifies said administrator's signature;
a vote list generating device which, if the verification of said administrator's signature is successful, generates a list of said vote data received from each said voter device and publishes it to make it accessible to said voters;
a decryption device which decrypts said information containing encrypted vote content with the secret key corresponding to said public key to obtain the voters' vote content; and
a counting device which counts up the votes for candidates based on said decrypted vote content.

{Claim 22} A counter device as per Claim 21 which comprises multiple distributed counter devices connected in series, each administered by a different counter, wherein said secret key is split up among said multiple distributed counter devices and assigned as a distributed secret key to each of them; the vote data sent from each said voter device is received by a distributed counter device at one end of said series; said distributed counter devices each comprise a distributed decryption processing unit, which units in series successively perform decryption processing of said information containing encrypted vote content using said distributed secret key assigned to each of them; and said vote content is obtained by means of decryption processing by said distributed decryption processing unit in said distributed counter device which is at the final stage.

{Claim 23} A counter device as per Claim 21 which comprises multiple distributed counter devices, each administered by a different counter, wherein said secret key is split up among said multiple distributed counter devices and assigned as a distributed secret key to each of them; each distributed counter device receives said vote data from all said voter devices and comprises a distributed decryption processing unit, each of which performs decryption processing of said encrypted vote content using said assigned distributed secret key to generate intermediate decrypted data, and sends it to a predetermined one

said distributed counter device; and said predetermined one said distributed counter device comprises a combination decryption unit which performs decryption processing of all gathered said intermediate decrypted data to obtain said vote content.

{Claim 24} A counter device as per Claim 22 or 23, wherein said distributed decryption processing unit performs thresholded decryption processing whereby decryption is possible when at least a predetermined number of two or more of said distributed counter devices is operating.

{Claim 25} A recording medium which records a program whereby a computer executes the processing procedure of a voter device in an electronic voting system which comprises multiple voter devices, an administrator device connected to each of said voter devices via a named communication channel, and a counter device connected to each of said voter devices via an anonymous communication channel, wherein said processing procedure comprises the following steps:

- (a) encrypting the vote content with the public key of a counter device to generate encrypted vote content;
- (b) generating a random number;
- (c) randomizing information containing said encrypted vote content with said random number to generate a preprocessed text;
- (d) generating a signature for said preprocessed text;
- (e) transmitting said preprocessed text and its signature to an election administrator device;
- (f) removing the effect of said random number from said administrator's blind signature for said preprocessed text received from the election administrator device using said random number to determine said administrator's signature for said information containing encrypted vote content;
- (g) verifying the authenticity of said information containing encrypted vote content;
- (h) if said verification of authenticity is successful, transmitting said information containing encrypted vote content and said administrator's signature as vote data to the counter device; and
- (i) verifying that one's own vote data is present in the vote list received from said counter device.

{Claim 26} A recording medium as per Claim 25, wherein the processing procedure additionally comprises the step of generating a tag known only to said voter, and a step of associating said encrypted vote content and said tag to generate said information containing encrypted vote content, wherein said step (i) comprises the step of extracting said tag from each vote datum in said vote list received from said counter device and examining if that tag is one's own to verify whether one's own vote data is present in said vote list.

{Claim 27} A recording medium which records a program whereby a computer executes the processing procedure of a counter device in an electronic voting system which comprises multiple voter devices, an administrator device connected to each of said voter devices via a named communication channel, and a counter device connected to each of said voter devices via an anonymous communication channel, wherein said processing procedure comprises the following steps:

- (a) accepting as input the information containing encrypted vote content encrypted with the counter's public key and the administrator signature for said information containing encrypted vote content, which are received as vote data from each said voter device, and verifying said administrator

signature;

(b) if verification of said administrator signature is successful, generating a list of said vote data received from each said voter device as a vote list and publishing that vote list to make it accessible to the voters;

(c) decrypting said information containing encrypted vote content using the secret key corresponding to said public key to obtain the voters' vote content; and

(d) counting up the votes for candidates based on said decrypted vote content.

{Claim 28} A recording medium as per Claim 27, wherein said counter device comprises multiple distributed counter devices connected in series, each administered by a different counter; said secret key is split up among said multiple distributed counter devices and assigned as a distributed secret key to each of them; said step (c) comprises the step of receiving said vote data sent from each said voter device by a distributed counter device at one end of said series and in series successively performing distributed decryption processing of said information containing encrypted vote content using said assigned distributed secret key, with said vote content being obtained by means of distributed decryption processing by said distributed decryption processing unit in said distributed counter device which is at the final stage.

{Claim 29} A recording medium as per Claim 27, wherein said counter device comprises multiple distributed counter devices connected in series, each administered by a different counter; said secret key is split up among said multiple distributed counter devices and assigned as a distributed secret key to each of them; and said step (c) comprises the step of receiving said vote data from all said voter devices at each distributed counter device, performing decryption processing of said encrypted vote content using said assigned distributed secret key to generate intermediate decrypted data, and sending it to a predetermined one said distributed counter device, whereby said one predetermined said distributed counter device performs combination decryption processing of all gathered said intermediate decrypted data to obtain said vote content.

{Claim 30} A recording medium as per Claim 28 or 29, wherein said step (c) performs thresholded distributed decryption processing whereby decryption is possible when at least a predetermined number of two or more of said distributed counter devices is operating.

{Detailed description of the invention}

{0001}

{Technical field of the invention} This invention relates to electronic voting systems, voting methods and program recording media intended to implement secure anonymous voting in cases of conducting questionnaires and the like via an electronic communication system.

{0002}

{Prior art} Voting is a process whereby each voter selects a predetermined number (one or more) of candidates from among multiple candidates presented to all the eligible voters and provides the results of that selection to a counter, who counts up the number of votes for each candidate. The candidates may be not only the names of candidates in a political election, but also choices in a statistical survey. Furthermore, the vote content is identifying information, symbols, names, items, etc. which represent the candidates selected by a voter.

{0003} Anonymous voting allows the correspondence between voter and vote content to be kept secret and is suited for protecting privacy with respect to an individual's ideas and beliefs, and thus can be used in electronic conferences, surveys conducted via duplex communication such as CATV, and so forth.

{0004} In order to conduct secure anonymous voting via electronic communication, it is necessary to prevent voter impersonation, duplicate votes, leaking of vote content or the like due to vote content eavesdropping, etc. Electronic voting schemes using digital signatures have been proposed as method of solving these problems, and are presented for instance in Atsushi Fujioka, Tatsuaki Okamoto, Kazuo Ohta: "A practical secret voting scheme for large scale elections", in Advances in Cryptology-AUSCRYPT '92, Lecture Notes in computer Science 718, Springer-Verlag, Berlin, pp. 244-251 (1993) and Japanese Patent Application Publication 6-19943 (published 28 November 1994) "Electronic voting method and apparatus".

{0005} In this prior art method, the voter V_i encrypts the vote content v_i with a key k_i to create an encrypted text x_i ; as preprocessing to obtain a blind signature therefore, x_i is randomized with a random number r_i to generate a preprocessed text e_i ; the voter's signature s_i is appended to the preprocessed text e_i and it is transmitted to an election administrator A. The election administrator A, after authenticating the legitimacy of the voter V_i based on the signature s_i , appends a the election administrator's blind signature d_i to the preprocessed text e_i and returns it to the voter. The voter V_i obtains the signature y_i of the election administrator A for the encrypted text x_i from the blind signature d_i for the preprocessed text e_i , and transmits it together with the encrypted text x_i to a counter C. The counter C confirms that the encrypted text x_i has been signed by the election administrator A and publishes a summary containing the encrypted text x_i as is. The voter V_i , if his own encrypted text x_i has been recorded, sends the key k_i used to encrypt the vote content v_i to the counter C, and if it has not been recorded, files an objection with the counter C. The counter C uses the key k_i received from the voter to decrypt the vote content v_i from the encrypted text x_i and counts it.

{0006}

{Problem to be solved by the invention} However, with this method, the voter V_i needs to confirm that his own encrypted text x_i was recorded from the vote summary published after the voting deadline and transmit the key k_i to the counter C, i.e., it is a system with low voter convenience.

{0007} The purpose of this invention is to provide a convenient electronic voting system and method which allows objections to be filed without infringing on privacy and makes it possible to handle counter improprieties and malfunctions and which does not require the voter to send the key used for encryption to the counter after voting.

{0008}

{Means of solving the problem} In this invention, a voter encrypts the vote content with the public key of a counter, further randomizes that encrypted vote content with a random number to generate preprocessed text, attaches a signature to that preprocessed text and transmits it to an election administrator. The election administrator, after authenticating the legitimacy of the voter using the attached signature, makes a blind signature to the preprocessed text and returns the blind

signature for the preprocessed text to each voter. The voter removes the effect of the random number from the blind signature for the preprocessed text to find the election administrator's signature information for the encrypted vote content, and transmits it together with the

encrypted vote content as vote data to the counter. The counter, after confirming that the signature information for the received encrypted vote content has been signed by the election administrator, publishes the vote data. After each voter has confirmed that his own encrypted vote content has been recorded in the published vote data list, the counter uses a secret key kept by him to extract the vote content from the encrypted vote content, and counts it up. If the encrypted vote content was not recorded in the vote list, an objection is filed against the counter. Furthermore, there may also be multiple counters, each holding a portion of the decryption key, whereby all the vote content is extracted from encrypted vote content by the cooperation of all or a specified number of counters.

{0009} According to this invention, in the encrypted vote content, the vote content is randomized with a random number, so the election administrator and counter cannot find the vote content from the randomized vote content, making it possible to ensure anonymity of the vote.

{0010} Here, the decryption key is held by the counter, and the voter does not need to again communicate with the counter for the purpose of opening the ballot.

{0011} If there are multiple counters, when vote content is opened through their cooperation, the fact that one is a legitimate voter can be indicated upon filing an objection simply by sending the encrypted vote content and the election administrator's signature. That is, even if a fraudulent person is present among the multiple counters, the vote content cannot be known unless all or a specified number of counters cooperate.

{0012} Furthermore, since encrypted vote content goes to distributed counters, here as well, unless all or a specified number of them cooperate, the midway progress of voting cannot be found out while voting is still going on, making for a fair voting scheme.

{0013} Moreover, in cases whether opening of votes is possible by the cooperation not of all but of a specified number of counters, even if some of the counters should be fraudulent or become unable to cooperate in opening votes, the vote opening operation can be properly carried out, so this scheme can be said to provide for a highly fault tolerant system.

{0014}

{Modes of embodiment of the invention} In the following embodiment examples, cases are described where this invention is applied to voting in a political election as an example of voting, but as discussed above, the voting principle envisioned by this invention can also be applied as is to voting in statistical surveys.

Embodiment example No. 1

Figure 1 is a drawing which shows the overall constitution of the voting system according to this invention. The devices 100 of T voters V_i ($i=1, \dots, T$) (called voter devices) are connected to the device 200 of the election administrator A (called election administrator device) and the device 300 of the counter C (called counter device) via named communication channels 400 and anonymous communication channels 500, respectively. When a voter V_i transmits information via a named communication channel 400 to the election administrator A,

sender information indicating who the sender is, for example a name V_i or identification information ID_i , is appended to the information transmitted, while when transmitting information via an anonymous communication channel to the counter C, sender information is not appended to the information transmitted. Furthermore, the counter C publishes a summary of vote content (vote list and polling score list), which the voters are all able to access. Figure 3 shows an example of the constitution of the voter device 100 in the voting system of Figure 1, Figure 4 shows an example of the constitution of an election administrator device 200, Figure 5 shows an example of the constitution of a counter device 300, and Figure 6 shows an example of the communication sequence in the voting system of this invention. Furthermore, Figure 2A illustrates an eligible voter list 240A possessed by the election administrator A, Figure 2B — a list of voters 240B given approval to vote, Figure 2C — a vote list 320A prepared by the counter C after the casting but before the counting of votes, Figure 2D — an example of a vote list 320A after counting, and Figure 2E — a polling score list 320B.

{0015} Below, the case is described wherein a voter V_i , after obtaining approval to vote from the election administrator A, performs the voting procedure with respect to the counter C.

{0016} The notation used in the following description is summarized here.

{0017} $x = \xi_C(v, k_{PC})$: the encryption function of counter C (x : encrypted text, v : vote content, k_{PC} : the counter's public key)
 $V = \rho_C(x, k_{SC})$: the decryption function of counter C (k_{SC} : the counter's secret key)

$s = \sigma_i(e)$: the signature generating function of voter V_i (s : signature, e : encrypted vote content)

$e = \zeta_i(s)$: the verification function for the signature of voter V_i

$d = \sigma_A(e)$: the blind signature generating function of the election administrator A (d : blind signature)

$z = \zeta_A(y)$: the verification function for the signature of the election administrator A (y : signature, z : ballot)

$e = \omega_A(z, r)$: randomization function (r : random number)

$y = \delta_A(d, r)$: random number component elimination function (d : blind signature)

Here, the encryption function ξ_C and the decryption function ρ_C of the counter C are ones used in well known public key cryptosystems; the counter C keeps the secret key k_{SC} secret and publishes the public key k_{PC} to the voters. Furthermore, the randomization function $\omega_A(z, r)$ for blinding (preprocessing for blind signing) with random number r the message m to be signed when the voter requests a blind signature, and the random number component elimination function $\delta_A(d, r)$ which removes the random number component r from the received blind signature d to extract the signature y of the election administrator A for the ballot z , are necessarily determined by the blind signature function σ_A used by the election administrator A. Such signature functions include for instance RSA cryptography encryption functions and decryption functions (Ronald Rivest, Adi Shamir, Leonard Adleman: "A method for obtaining digital

signatures and public-key cryptosystems", Communications of the ACM, vol. 21, No. 2, pp. 120-126 (Feb., 1978)), and details regarding techniques of randomization with random numbers as preprocessing for requesting a blind signature are described in David Chaum: "Security without identification: Transaction systems to make big brother obsolete", Communications of the ACM, Vol. 28, No. 10, pp. 1030-1044 (Oct., 1985).

{0018} The voter device 100 shown in Figure 3 is constituted as follows. A memory 121 stores in advance the voter's identification information ID_i and name V_i. Furthermore, data which is generated in the device 100 and used in subsequent processing is also stored in the memory 121. The encryption device 110 encrypts the vote content v_i selected by the voter V_i (here, for instance, candidate name CND_i) with the public key k_{PC} of the counter C and obtains an encrypted text x_i = ξ_C(v_i, k_{PC}). The tag generating device 111 generates a random number t_i, which is used as a tag known only to voter V_i, as described below. The associating device 112 associates the encrypted text x_i and the tag t_i and outputs z_i = x_i || t_i. Hereinafter, z_i will be called a ballot. The random number generating device 120 generates a random number r_i. The randomization device 130 randomizes the ballot z_i with random number r_i by means of a randomization function e = ω_A(z, r) as preprocessing for blind signing and generates a preprocessed text e_i. The signature generating device 140 generates a signature s_i = σ_i(e_i, ID_i) for the preprocessed text e_i to indicate that it belongs to the voter V_i. The data <e_i, s_i, ID_i> is transmitted from the transmission and reception unit 190 via a communication line 400 to the election administrator device 200. The connection with the election administrator device 200 via the communication line 400 is maintained until a blind signature d_i is received from the election administrator device 200.

{0019} The random number component elimination device 150 removes the random number component from the blind signature d_i received via the transmission and reception unit 190 from the election administrator device 200 by means of the random number component elimination function y_i = δ_A(d_i, r_i) using the random number r_i, and obtains y_i as the signature of the election administrator A for the ballot z_i. The signature verification unit 160 examines whether or not the verification function z_i = ζ_A(y_i) holds true to verify if y_i is authentic. The data <z_i, y_i> is transmitted from the transmission and reception unit 180 to the counter device 300. The list inspection part 170 accesses the counter device 300 and inspects the vote list 320A obtained via the transmission and reception unit 180.

{0020} The election administrator device 200 shown in Figure 4 has a memory 240 for recording an eligible voter list 240A (Figure 2A) with identification information ID_i of eligible voters prerecorded therein, and a voter list 240B (Figure 2B) in which identifications ID_i of voters who have been given approval to vote are written; a voter verification unit 210 which checks whether identification information ID_i received from a voter is on the eligible voter list; a signature verification unit 220 which verifies the correctness of a voter's signature s_i for the voter's preprocessed text e_i received based whether or not the verification function e_i = ζ_i(s_i) holds true; a voter list generation unit 260 which writes legitimate voters into a specific region of memory 240 to generate a voter list; a signature generating device 230 which generates a blind signature d_i = σ_A(e_i) for the preprocessed text e_i; and a transmission and reception unit 250

which performs transmission and reception of data to and from voter devices.

{0021} The counter device 300, as shown in Figure 5, has a signature verification unit 310 which verifies the signature y_i by checking whether or not z_i = ζ_A(y_i) holds true using the verification function ζ_A(y_i) on the ballot z_i and the signature y_i of the election administrator A in the vote data <z_i, y_i> received via the transmission and reception unit 360 from a voter device 100; a memory 320 which stores the vote list 320A (Figure 2C) with a serial number q_i affixed to the vote data <z_i, y_i> by the vote list generating unit 370 added thereto; a separation unit 350 which separates the encrypted text x_i from the ballot z_i = x_i || t_i; a decryption device 330 which decrypts x_i by means of the decryption function p_C using the counter's secret key k_{SC} to obtain v_i = p_C(x_i, k_{SC}) as the vote content; and a counting device 340 which counts up the vote content v_i. Furthermore, decrypted vote content v_i is added to the vote data corresponding to serial number q of the vote list 320A stored in memory 320, as shown in Figure 2D. The count results are stored in memory 320 as a polling score list 320B of the number of votes C_h (h = 1, 2, ...) obtained by each candidate (CND_h; h = 1, 2, ...), as shown in Figure 2E. The content of the vote list 320A and polling score list 320B are transmitted to voter device 100 making access through the transmission and reception unit 380.

{0022} Below, the voting procedure in this embodiment example No. 1 is described with reference to Figure 6.

Step S1: A voter V_i performs preparation for voting using the voter device 100 (Figure 3) as follows.

{0023} Step S1-1: The voter V_i encrypts the vote content v_i with the encryption device 110 using the secret key k_{PC} of the counter C and the encryption function ξ_C to generate encrypted text x_i = ξ_C(v_i, k_{PC}).

Furthermore, he generates a tag t_i using the tag generating device 111 and associates it with x_i using the associating device 112 to obtain a ballot z_i = x_i || t_i.

The tag t_i is for instance a random number, and only the voter V_i knows that it is his.

{0024} Step S1-2: The voter V_i generates a random number r_i using the random number generating device 120 and randomizes z_i with r_i using the randomization device 130 to generate preprocessed text e_i = ω_A(z_i, r_i).

{0025} Step S1-3: The voter V_i uses the signature generating device 140 to generate a signature

s_i = σ_i(e_i, ID_i) for the preprocessed text e_i and the identification information ID_i, and transmits the data <e_i, s_i, ID_i> from the transmission and reception unit 190 to the election administrator device 200.

Step S2: The election administrator device 200 (Figure 4) possesses in advance the relationships between registered eligible voter names V_i and their identification information ID_i, as shown in Figure 2A, in the form of an eligible voter list 240A (Figure 2A), and also has a voter list 240B (Figure 2B) for writing in, by means of the voter list generating unit 260, the name V_i or identification information ID_i of eligible voters given approval to vote. The voter list is published after acceptance of votes is completed; if it is permissible to publish the names V_i of approved voters, the voter name V_i is written in, while if it is being avoided that the names of voters should

become known, the identification information ID_i is written in. One of these is decided upon for the voting system. In the description below, the identification information ID_i of the voter V_i will be written in the voter list 240B (Figure 2B). Upon commencement of vote acceptance, there is nothing recorded in the voter list. The approval procedure by the election administrator device 200 is carried out as follows.

{0026} Step S2-1: The election administrator A confirms that a voter is an eligible voter by checking if his identification information ID_i is present in the eligible voter list 240A (Figure 2A) by means of the voting eligibility confirmation unit 210. If it is not, the election administrator A denies the approval.

{0027} Step S2-2: The election administrator A checks whether the voter V_i has previously received approval from the election administrator A by examining if his ID_i has already been entered in the voter list 240B (Figure 2B) by means of the vote eligibility confirmation unit 210. If the ID_i has already been given approval, the election administrator A denies approval as a case of duplicate voting.

{0028} Step S2-3: If ID_i has not been entered previously, the election administrator verifies that s_i , e_i and ID_i satisfy the following formula

$$(e_i, ID_i) = \zeta_A(s_i)$$

using the signature verification device 220. If verification is successful, the election administrator A computes, via the signature generating device 230, the signature d_i

$$d_i = \sigma_A(e_i),$$

transmits d_i from the transmission and reception unit 250 to the voter device 100, and adds the ID_i of voter V_i to the voter list 240B (Figure 2B) in memory 240 by means of the voter list generating unit 260.

{0029} Step S2-4: After acceptance of votes has ended, the election administrator A publishes the voter list 240B and the number of voters. As for the method of publication, notice is given in advance to eligible voters that the voter list 240B in the memory 240 of the election administrator device 200 can be accessed via arbitrary communication channels within a specified period of time from a specific date. The method of access to this list can be implemented for instance by means of a predetermined telephone number. The place of publication of voter list 240B may also be a predetermined internet address, rather than inside the election administrator device 200.

Step S3: The voter V_i generates the ballot and corresponding signature information using the voter device 100 (Figure 3) as follows.

{0030} Step S3-1: The voter V_i inputs d_i and r_i into the random number component elimination device 150 to obtain the signature information y_i for the ballot z_i

$$y_i = \delta_A(d_i, r_i)$$

{0031} Step S3-2: The voter V_i uses the signature verification device 160 to confirm that y_i is the signature of the election administrator A based on whether or not

$$z_i = \zeta_A(y_i)$$

holds true. If it does not, the voter V_i claims impropriety on the part of the election administrator A by presenting the data $\langle e_i, d_i \rangle$.

{0032} Step S3-3: If said signature confirmation succeeds, the voter V_i transmits the data $\langle z_i, y_i \rangle$ from the transmission and reception unit 180 to the counter device 300 via communication channel 500.

Step S4: The counter C collects votes using the counter device 300 as follows.

{0033} Step S4-1: The counter C receives vote data $\langle z_i, y_i \rangle$ from voters via reception unit 360 and uses the signature verification device 310 to confirm that y_i is an authentic signature for the ballot z_i by verifying whether or not

$$z_i = \zeta_A(y_i)$$

holds true. If the verification succeeds, the ballot z_i and its signature y_i are numbered with a serial number q and entered as vote data $\langle q, z_i, y_i \rangle$ into the voter list 230A (Figure 2C) by means of the vote list generating unit 370.

{0034} Step S4-2: After all votes have been cast, the counter C publishes a vote list 320A by enabling access to the memory 320 via the transmission and reception unit 380. This vote list is made accessible to all voters. For the publication method, advance notice is given of the publication period and publication location, just as in the case of voter list 240B discussed above.

Step S5: The voter V_i performs verification using the voter device 100 as follows.

{0035} Steps S5-1: The voter V_i accesses the memory 320 of the counter device 300 by means of the transmission and reception unit 180, receives the content of the voter list 320A and verifies that the number of votes listed in the voter list 320A is equal to the voter list published in Step 2-4 by means of the list verification device 170. If it does not match, number q and random number r is published, and a claim of impropriety is filed with the election administrator A.

{0036} Steps S5-2: Voter V_i verifies that his own ballot z_i has been published in the voter list 320A by means of the list verification device 170. For the verification, one may verify whether z_i itself is present in the list, or verify that the tag t_i in $z_i = x_i \parallel t_i$ is one's own. If it has not been published, a claim of impropriety on the part of the counter C is made by presenting the vote data $\langle z_i, y_i \rangle$.

Step S6: The counter C opens and counts votes by means of the counter device 300 as follows.

{0037} Step S6-1: After commencement of reception of ballots z_i and signatures y_i from voters V_i using the reception unit 360, if there are no notices of aforesaid impropriety within a specific period of time, the counter C separates x_i the ballot $z_i = x_i \parallel t_i$ with the separation unit 350, opens the ballot with the decryption device 330, uses the secret key k_{SC} to determine the vote content v_i based on

$$v_i = \rho_C(x_i, k_{SC}),$$

and verifies that the vote content v_i is a correct vote, i.e. that the vote content v_i comprises names or symbols representing candidates presented in advance. If not, it is considered to be an invalid vote.

{0038} Step S6-2: The counter C counts up the vote content v_i in the voter list of Figure 2C using the counting device 340, obtains the number of votes cast for each candidate, publishes the result as a polling score table 320B shown in Figure 2E, and adds v_i for the qth vote datum $\langle x_i, t_i, y_i \rangle$ as shown in Figure 2D. The count results are appended to the vote list 320A and published.

Step S7: The voter V_i confirms that the operations of the counter C are correct by means of the voter device 100. That is, he confirms if all of v_i has been added to the voter list 320A shown in Figure 2C and if it corresponds to x_i and v_i of the voter V_i .

{0039} The aforementioned step S5 may be omitted. Furthermore, the publication of the polling score list in step S6-2, as well as step S7, may also be omitted.

{0040} In the embodiment described above, the voter V_i encrypts the vote content v_i using the encryption function ξ_C of the counter C as $x_i = \xi_C(v_i, k_{PC})$ and sends the vote data $\langle z_i, y_i \rangle$ to the counter C, so the counter C, if he so intends, can decrypt x_i in z_i by means of the decryption function $v_i = \rho_C(x_i, k_{sc})$ using the counter's secret key k_{PC} to obtain v_i before the vote list is published in Step 4-2. That is, he can obtain information such as the voting trend or the midway results without waiting for publication of the vote list and leak that information to particular persons before the official count results come out, which is undesirable with respect to the fairness of an election. Furthermore, in embodiment example No. 1, if the counter device 300 breaks down, it may not be possible to complete vote counting on schedule. Below, an embodiment example is described which improves these points by decrypting and counting the encrypted vote content with multiple counter devices administered by multiple counters.

{0041} Here, the cryptographic functions (encryption function ξ_C and decryption function ρ_C) of the distributed counters are used by means of a public key cryptography scheme, with decryption of the encrypted text becoming possible only when decryption processing for each encrypted text x_i has been performed with the distributed decryption keys k_{SCj} held by all the distributed counters, or else there is a threshold U_t ($2 < U_t < U$) for the number of persons required for decryption, with decryption being possible when the specified number of threshold distributed counters comes together. Such cryptographic functions include for example the encryption and decryption functions of ElGamal cryptography (Taher ElGamal: "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, Vol. IT-31, No. 4, pp. 469-472 (July, 1985)); details on techniques of decryption by distributed decryptors and techniques employing a threshold are described in Yvo Desmedt, Yale Frankel: "Threshold cryptosystems" in Advances in Cryptology-CRYPTO '89, Lecture Notes in Computer Science 435, Springer-Verlag, Berlin, pp. 307-315 (1990).

Embodiment example No. 2

Figure 7 shows the overall constitution of a voting system according to embodiment example No. 2. In this embodiment example, the point that the voter devices 100 are each connected to an election administrator device 200 via a communication

channels 400 and are each connected to one counter device via a communication line 500 is the same as in embodiment example No. 1; the point of difference in constitution is that multiple counter devices 300_j ($j = 1, \dots, U$; hereinafter called distributed counter devices) are provided, whereby the distributed counter device 300₁ performs decryption processing of the encrypted text x_i from all voters to generate x_{i1} , which is sent to the next distributed counter device 300₂, with the jth distributed counter device 300_j similarly performing decryption processing of the decryption processed data x_{ij-1} , received from the immediately preceding distributed counter device 300_{j-1}, to generate x_{ij} , and sending it to the next distributed counter device 300_{j+1}. The vote content v_i is first obtained through decryption processing by the final distributed counter device 300_U. Just as in embodiment example No. 1, when a voter device 100_i sends data to the administrator device 200 via communication channel 400, the identification information ID_i of the voter V_i is appended thereto, while no identification information ID_i is appended when sending data to the distributed counter device 300₁ via communication channel 500.

{0042} Except for the fact that the counter device 300 is made into distributed counter devices 300, the communication sequence example, the example of the constitution of each voter device 100_i, the example of the constitution of the election administrator device 200, etc. are the same as before. Furthermore, the point that each voter uses a common public key k_{PC} to encrypt the vote content v_i by means of $x_i = C(v_i, k_{PC})$ is the same as in embodiment example No. 1; however, each of the counters C₁ to C_U has a distributed secret key $k_{SC1}, k_{SC2}, \dots, k_{SCU}$, a U number of which are generated from the secret key k_{SC} , which are used to perform decryption processing, and the vote content v_i cannot be decrypted from the encrypted text x_i by any counter device 300_i alone. When the aforementioned ElGamal cryptography is used as the cryptosystem, such distributed secret keys $k_{SC1}, k_{SC2}, \dots, k_{SCU}$ can for instance be determined such that the sum of the values of these keys will be equal to the value of the secret key k_{SC} corresponding to the public key k_{PC} , as indicated in the aforementioned document of Desmedt-Frankel.

{0043} Figure 8A shows the constitution of the first distributed counter device 300₁ which gathers votes from the voter devices 100₁ to 100_T and which comprises a signature verification unit 310, a memory 320, a counting device 340, a separation unit 350, a distributed decryption processing unit 331, reception unit 360, a vote list generating unit 370 and a transmission and reception unit 380. It differs from the counter device 300 of embodiment example No. 1 shown in Figure 5 in the following respects. First, decryption processing $x_{i1} = \rho_{C1}(x_i, k_{SC1})$ using distributed secret key k_{SC1} is performed on encrypted text x_i in the distributed decryption processing unit 331 to generate intermediate decrypted data x_{i1} , which is sent to the next distributed counter device 300₂. Second, the counting device receives decrypted vote content v_i from the final distributed counter device 300_U and counts it. The 2nd through the Uth distributed counter devices 300₂ to 300_U, as shown in Figure 8B represented by the jth distributed counter device ($2 \leq j \leq U$), only have a distributed decryption processing unit 331, performing decryption processing $x_{ij} = \rho_{Cj}(x_{ij-1}, k_{SCj})$ using the distributed secret key k_{SCj} on the intermediate decrypted data x_{ij-1} received from the preceding distributed counter device 300_{j-1} to

generate intermediate decrypted data x_{ij} , which is transmitted to the following distributed counter device 300_{j+1} . However, at the final distributed counter device 300_U , x_{iU} can be obtained as the final decryption result, which is the vote content $v_i = x_{iU}$, by means of decryption processing $x_{iU} = \rho_{CU}(x_{iU-1}, k_{SCU})$, and that vote content v_i is transmitted to the first distributed counter device 300_1 .

{0044} The voting procedure in this embodiment example No. 2 will be described. In this embodiment example, the same procedure is performed as the procedure from step S1 to Step S5 in embodiment example No. 1. However, the vote data $\langle z_i, y_i \rangle$ from each voter device 100_i is received by the first distributed counter device 300_1 . In this embodiment example No. 2, steps S6 and S7 of embodiment example No. 1 are modified as follows, U being the number of distributed counter devices.

Step S6: Distributed counter C_j ($j = 1, \dots, U$) performs counting by means of distributed counter device 300_j as follows.

{0045} Step S6-1: The first distributed counter device 300_1 separates $z_i = x_i \parallel t_i$ in the vote data $\langle z_i, y_i \rangle$ from each voter device 100_i ($i = 1, \dots, T$) into encrypted text x_i and tag t_i with the separation unit 350, performs the following decryption processing

$$x_{ii} = \rho_{C1}(x_i, k_{SC1})$$

by means of the distributed decryption processing unit 330 using the distributed secret key k_{SC1} , obtains intermediate decrypted data x_{ii} and sends it to the next, 2nd distributed counter device 300_2 .

{0046} Thereafter similarly, the jth distributed counter device 300_j performs decryption processing

$x_{ij} = \rho_{Cj}(x_i, k_{SCj-1})$ on intermediate decrypted data $x_{i(j-1)}$ from the $(j-1)$ th distributed counter device 300_{j-1} by means of the distributed decryption processing unit 330 using the distributed secret key k_{SCj} , and sends the obtained intermediate decrypted data x_{ij} to the next, $(j+1)$ th distributed counter device 300_{j+1} .

{0047} The final Uth distributed counter device 300_U performs decryption processing

$v_i = x_{iU} = \rho_{CU}(x_i, k_{SCU})$ on the intermediate decrypted data x_{iU-1} from the $(U-1)$ th distributed counter device by means of the distributed decryption processing unit 330 using the distributed secret key k_{SCU} to obtain the vote content v_i . The Uth distributed counter device 300_U verifies whether or not the obtained vote content is invalid.

{0048} Step S6-2: The Uth distributed counter C_U counts the vote content v_i using the counting device 340, publishes the results thereof, and adds the vote content v_i to the vote list.

Step 7: The voter V_i confirms that the operation of the distributed counter device 300_U is correct by means of the voter device 100_i .

{0049} In this way, in embodiment example No. 2, since decryption processing is performed sequentially by multiple distributed counter devices 300_1 to 300_U and the vote content v_i is obtained at the final distributed counter device 300_U , no distributed counter alone can open votes and obtain v_i before the start of counting.

Embodiment example No. 3

Figure 9 shows the overall constitution of the voting system of embodiment example No. 3. In this embodiment example, each voter device 100_i ($i = 1, \dots, T$) is able to connect via communication lines 500 to all of the distributed counter devices 300_1 to 300_U , and sends the generated vote data $\langle z_i, y_i \rangle$

to all the distributed counter devices 300_1 to 300_U . The constitution of each voter device 100_i and of the election administrator device 200 is the same as in embodiment examples No. 1 and No. 2.

{0050} The constitution of the 1st to the $(U-1)$ th distributed counter device 300_1 to 300_{U-1} , as shown in Figure 10A represented by the jth distributed counter device 300_j , comprises a signature verification unit 310 which performs verification of the signature y_i for z_i in the vote data received from each voter device 100_i , a separation unit 350 which separates the encrypted text x_i from z_i , and a distributed decryption processing unit 331 which performs decryption processing $x_{ij} = \rho_{Cj}(x_i, k_{SCj})$ using distributed decryption key k_{SCj} on the encrypted text to generate intermediate decrypted data x_{ij} , which is transmitted to a predetermined distributed counter device, in this example 300_U . Distributed counter device 300_U , as shown in Figure 10B, is constituted by adding a memory 320; combination decryption unit 332; counting device 340; a vote list generating unit 370 which appends a serial number q to each vote datum $\langle z_i, y_i \rangle$ collected from preceding distributed counter devices $300_1, \dots, 300_{U-1}$ and enters it into the vote list 320A; and a transmission and reception unit 380 which communicates with the voter device 100_i to make the vote list 320A and polling score list 320B accessible. In the memory 331, a vote list 320A which lists the received vote data and a polling score list 320B for each candidate representing the results of counting are formed. The combination decryption unit 332 performs decryption processing $v_i = \rho_C(x_{ii}, \dots, x_{iU})$ by means of decryption function ρ_C on intermediate decrypted data x_{ii} to x_{iU} generated by distributed counter devices 300_1 to 300_U to obtain vote content v_i , and supplies it to the counting device 340. The counting device 340 verifies the validity of the vote content v_i , and if it is valid, adds 1 to the polling score of the corresponding candidates in the polling score list generated in memory 320. Furthermore, it adds v_i to the corresponding vote data in the vote list.

{0051} In this embodiment example No. 3 as well, each distributed counter device cannot by itself decrypt the vote content v_i from the encrypted text x_i , thus ensuring fairness of the election.

Modified embodiment example 1

In embodiment examples No. 2 and No. 3, the vote content v_i cannot be decrypted from the encrypted text x_i unless all the distributed counters C_1 to C_U cooperate. However, for instance by forming the distributed decryption processing unit 331 according to the method of Desmedt-Frankel discussed above, it is possible to decrypt v_i from encrypted text x_i encrypted using public key k_C with at least L ($2 \leq L \leq U-1$) distributed counter devices. An embodiment example applying this method to embodiment example No. 2 (Figures 7, 8A and 8B) will be described.

{0052} For instance, even if one of the distributed counter devices 300_2 to 300_U , say, 300_j , break down, the immediately preceding distributed counter device 300_{j-1} avoids distributed counter device 300_j and sends intermediate decrypted data x_{ij-1} to distributed counter device 300_{j+1} . Distributed counter device 300_{j+1} uses distributed secret key k_{SCj+1} on the intermediate decrypted data x_{ij-1} according to $x_{ij+2} = \rho_C(x_i, k_{SCj+1})$ to obtain intermediate decrypted data x_{ij+1} , and can then just pass it on further to the following distributed counter device 300_{j+2} . The

method of generating the distributed secret key used in this case is indicated for instance in the aforementioned document by Desmedt-Frankel. Furthermore, if the constitution of all the distributed counter devices 300₁ to 300_U is made as the constitution shown in Figure 8A, even if the first distributed counter device 300₁ should break down, the next stage distributed counter device 300₂ can receive vote data <z_i, y_i> from voter devices 100₁ to 100_T instead of it, substituting in performing the functions of distributed counter device 300₁. It then suffices for the last stage distributed counter device 300_U to transmit the vote content v_i obtained through decryption processing to the substitute distributed counter device 300₂. According to this embodiment example, vote counting can be performed even if any number of distributed counter devices U-L or less should break down.

Modified embodiment example 2

Similarly, by applying the method of Desmedt-Frankel to the distributed decryption processing unit 331 and combination decryption unit in embodiment example No. 3 (Figures 9, 10A and 10B), v_i can be decrypted so long as intermediate decrypted data is obtained by L or more (2 ≤ L ≤ U-1) distributed counter devices out of the distributed counter devices 300₁ through 300_{U-L}. For example, if distributed counter devices 300₁ to 300_{U-L} broke down, the vote content v_i can be decrypted by providing the intermediate decrypted data x_{iU-L+1} to x_{iU} from the remaining distributed counter devices 300_{U-L+1} to 300_U to the combination decryption unit 332 of distributed counter device 300_U and applying decryption processing v_i = p_C(x_{iU-L+1}, x_{iU-L+2}, ..., x_{iU}) thereto. The validity of the obtained vote content v_i is verified by the counting device 340, and if valid, 1 is added to the polling score of the candidates corresponding to v_i in the polling score list in memory 320.

{0053} In this modified embodiment example, if the constitution of all the distributed counter devices 300₁ to 300_U is made the same as that shown in Figure 10B, even if any number of distributed counter devices U-L or less should break down, vote counting can be performed by having a remaining one perform the same operation as the distributed counter device in Figure 10B.

{0054} Each of the devices shown in Figures 3 to 5, 8A, 8B, 10A and 10B are shown in terms of their functional constitution; each of these functions can also be implemented by providing a control unit to cause the operations to be performed successively; furthermore all or part of them can be executed by a computer.

{0055}

{Effect of the invention} As described above, in this invention, the vote content v_i is encrypted with the counter's public key k_{P,C}, so there is no need for the voter to transmit a key to the counter in order to encrypt the vote content.

{0056} When there are multiple counters, the ballot opening

operation will not begin unless the agreement of all counters is obtained.

{0057} Furthermore, when a specified number of counters can open ballots, the ballot opening operation can be started once legitimate counters come together to a certain extent, allowing the effect of fraudulent persons or saboteurs to be eliminated.

{0058} Furthermore, even if a counter should tamper with the vote content, tampering with vote content can be detected by perusing the published summary of vote content. That is, when one's own vote was not used, it suffices to disclose the encoded ballot z_i and the election administrator's signature y_i and claim impropriety. Here, if there is a certain number of fraudulent counters, privacy when filing an objection is guaranteed.

{0059} Moreover, when multiple counters are provided, in this invention, since the vote content is transmitted encrypted, improprieties such as a counter leaking the midway progress to influence an election while ballots are being collected can be prevented.

{0060} As per the above, with this invention, voter convenience can be improved by using the counter's encryption key, and furthermore, by providing multiple counters, improprieties such as influencing an election by leaking the midway progress can be resolved.

{Brief description of the drawings}

{Figure 1} A block diagram showing the overall constitution of an election system according embodiment example No. 1 of this invention.

{Figure 2} A is a table showing an eligible voter list; B is a table showing a voter list; C is a table showing a vote list; D is a table showing a vote list; E is a polling score list.

{Figure 3} A block diagram showing an example of the functional constitution of a voter device 100.

{Figure 4} A block diagram showing an example of the functional constitution of an election administrator device 300.

{Figure 5} A block diagram showing an example of the functional constitution of a counter device 400.

{Figure 6} A diagram showing the vote processing procedure.

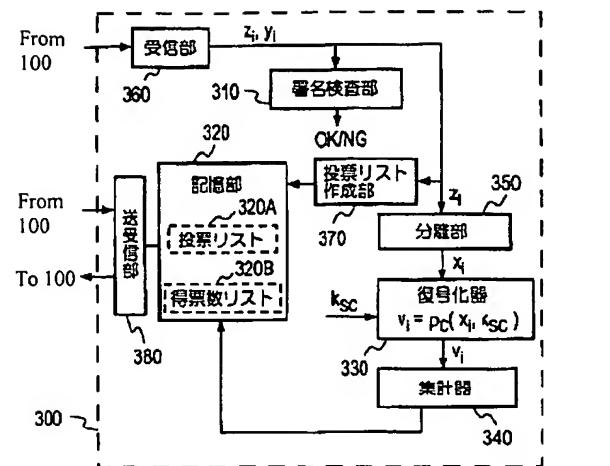
{Figure 7} A block diagram showing the overall constitution of an election system according to embodiment example No. 2.

{Figure 8} A is a block diagram showing an example of the functional constitution of distributed counter device 300₁ in Figure 7; B is a block diagram showing the functional constitution of distributed counter devices 300₂ to 300_U in Figure 7.

{Claim 9} A block diagram showing the overall constitution of a voting system according to embodiment example No. 3.

{Claim 10} A is a block diagram showing the functional constitution of distributed counter device 300₁ to 300_{U-1} in Figure 9; B is a block diagram showing the functional constitution of distributed counter device 300_U in Figure 9.

{Figure 5}



310: Signature verification unit
 320: Memory
 320A: Vote list
 320B: Polling score list
 330: Decryption device
 340: Counting device
 350: Separation unit
 360: Reception unit
 370: Vote list generating unit
 380: Transmission and reception unit

Figure 5

{Figure 7}

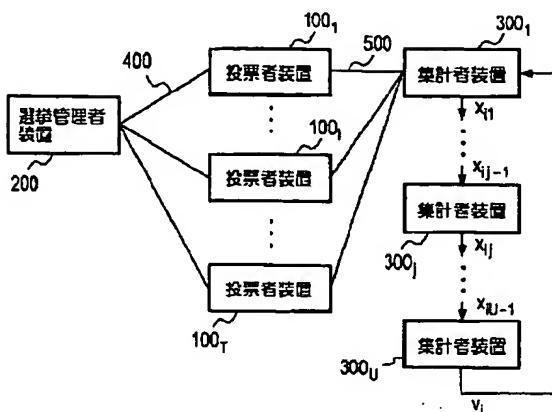
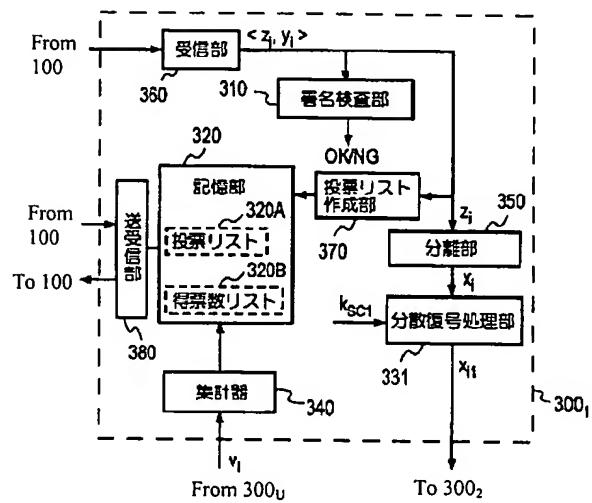


Figure 7

100₁, 100_i, 100_T: Voter device
 200: Election administrator device
 300₁, 300_j, 300_U: Counter device

{Figure 8}

A



B

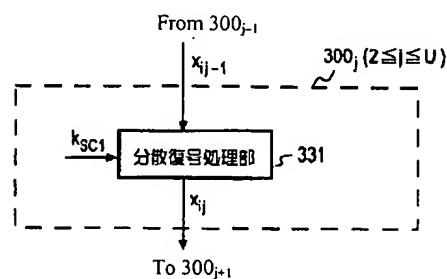


Figure 8

310: Signature verification device
 320: Memory
 320A: Vote list
 320B: Polling score list
 331: Distributed decryption processing unit
 340: Counting device
 350: Separation unit
 360: Reception unit
 370: Vote list generating unit
 380: Transmission and reception unit

{Figure 6}

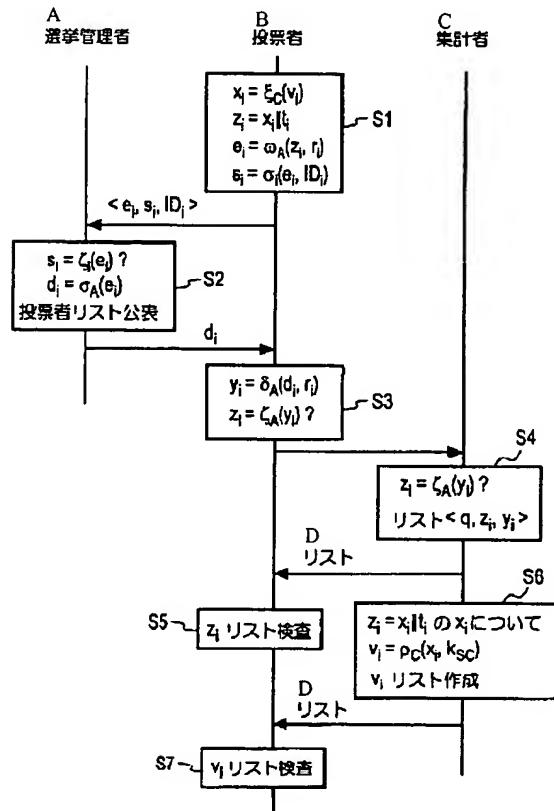


Figure 6

S2: Voter list publication
 S4: List <q, z_i, y_i>
 S5: z_i list verification
 S6: For x_i of z_i = x_i || t_i
 v_i = p_C(x_i, k_{SC})
 v_i list generation

S7: v_i list verification
 A: Election administrator
 B: Voter
 C: Counter
 D: List

{Figure 9}

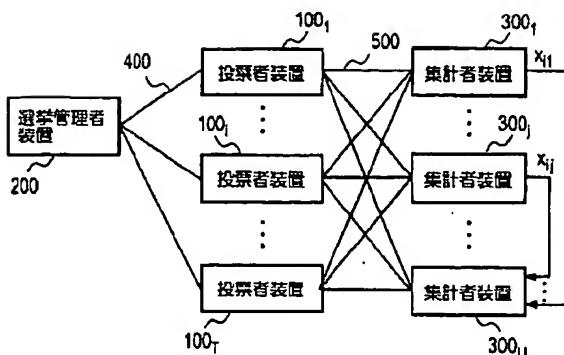


Figure 9

$100_i, 100_j, 100_T$: Voter device
 200 : Election administrator device
 $300_i, 300_j, 300_U$: Counter device

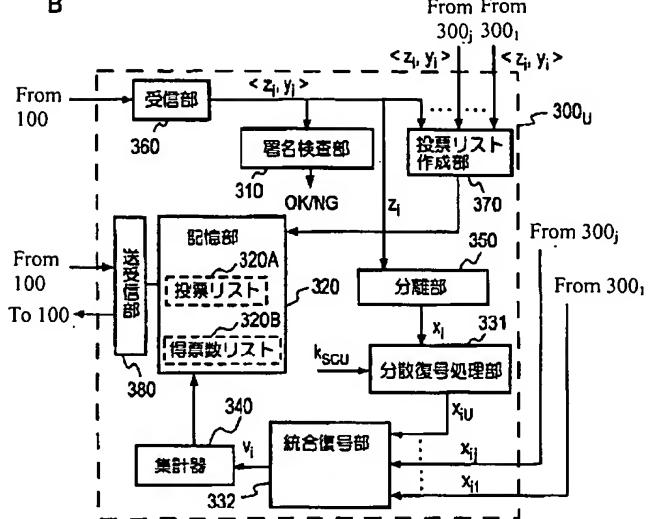
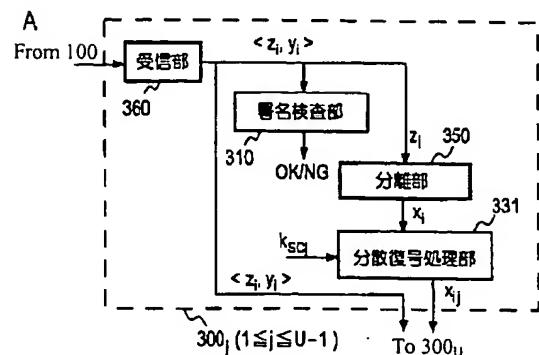


Figure 10

- 310: Signature verification device
- 320: Memory
- 320A: Vote list
- 320B: Polling score list
- 331: Distributed decryption processing unit
- 332: Combination decryption unit
- 340: Counting device
- 350: Separation unit
- 360: Reception unit
- 370: Vote list generating unit
- 380: Transmission and reception unit

{Amendment of proceedings}

{Submission date} 22 November 1999 (1999.11.22)

{Amendment of proceedings 1}

{Title of document amended} Specification

{Title of item amended} Claim 7

{Method of amendment} Modification

{Content of amendment}

{Claim 7}

An electronic voting method as per Claim 1 or 2, wherein said step (a) comprises the step of generating a voter signature for said preprocessed text and transmitting it together with said preprocessed text to said administrator device, and wherein said step (b) comprises the step of verifying the authenticity of said voter signature for said preprocessed text.